Accès à distance VPN ASA avec la vérification OCSP sous Microsoft Windows 2012 et OpenSSL

Contenu

Introduction

Ce document décrit comment utiliser la validation en ligne de Protocol d'état de certificat (OCSP) sur une appliance de sécurité adaptable Cisco (ASA) pour des Certificats présentés par des

utilisateurs VPN. Des exemples de configuration pour deux serveurs OCSP (autorité de certification de Microsoft Windows [CA] et OpenSSL) sont présentés. La section de vérifier décrit des écoulements détaillés au niveau de paquet, et la section de dépannage se concentre sur des erreurs et des problèmes typiques.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de l'interface de ligne de commande d'appliance de sécurité adaptable Cisco (CLI) et configuration du VPN de Protocole SSL (Secure Socket Layer)
- Certificats X.509
- Microsoft Windows Server
- Linux/OpenSSL

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel d'appliance de sécurité adaptable Cisco, version 8.4 et ultérieures
- Microsoft Windows 7 avec le Client à mobilité sécurisé Cisco AnyConnect, version 3.1
- Serveur 2012 R2 de Microsoft
- Linux avec OpenSSL 1.0.0j ou plus tard

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

> Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Le client utilise l'Accès à distance VPN. Cet accès peut être Client VPN Cisco (IPSec), mobilité sécurisée de Cisco AnyConnect (version 2 [IKEv2] de Key Exchange SSL/Internet), ou webvpn (portail). Afin d'ouvrir une session, le client fournit le certificat correct, aussi bien que le nom d'utilisateur/mot de passe qui ont été configurés localement sur l'ASA. Le certificat client est validé par l'intermédiaire du serveur OCSP.

Accès à distance ASA avec OCSP

L'ASA est configurée pour l'accès SSL. Le client emploie AnyConnect afin d'ouvrir une session. L'ASA emploie l'inscription de certificat simple Protocol (SCEP) afin de demander le certificat :

```
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
```

Une carte de certificat est créée afin d'identifier tous les utilisateurs dont le subject-name contient l'administrateur de mot (ne distinguant pas majuscules et minuscules). Ces utilisateurs sont liés à un groupe de tunnels nommé 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 configuration du VPN exige l'autorisation réussie (c'est-à-dire, un certificat validé). Il exige également les qualifications correctes pour le nom d'utilisateur localement défini (AAA d'authentification) :

```
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

> Remarque: Voir le guide de configuration de gamme de Cisco ASA 5500 utilisant le CLI, les 8.4 et les 8.6 : Configurer un serveur externe pour l'autorisation d'utilisateur de dispositifs de sécurité pour des détails sur la configuration de l'ASA par le CLI.

Installation de services

Cette procédure décrit comment configurer des services de rôle pour le serveur de Microsoft :

1. Naviguez vers le **gestionnaire du serveur > gèrent > ajoutent des rôles et des caractéristiques**. Le serveur de Microsoft a besoin de ces services de rôle :

   Autorité de certificationInscription de Web d'autorité de certification, qui est utilisée par le clientResponder en ligne, qui est nécessaire pour OCSPLe service d'inscription de périphérique de réseau, qui contient l'application SCEP l'a utilisé par l'ASA Le service Web avec des stratégies peut être ajouté si nécessaire.

2.
3.
4. Quand vous ajoutez des caractéristiques, soyez sûr d'inclure les outils en ligne de responder parce qu'il inclut un OCSP SNAP-dans cela est utilisé plus tard :

Configuration CA pour le modèle OCSP

Le service OCSP emploie un certificat pour signer la réponse OCSP. Un certificat spécial sur le serveur de Microsoft doit être généré et doit inclure :

- Utilisation principale étendue = signature OCSP
- OCSP aucun vérifier de révocation

Ce certificat est nécessaire afin d'empêcher des boucles de validation OCSP. L'ASA n'emploie pas le service OCSP pour essayer de vérifier le certificat présenté par le service OCSP.

1. Ajoutez un modèle pour le certificat sur le CA naviguent vers **CA > modèle de certificat > gèrent**, **réponse** choisie **OCSP signant**, et reproduisent le modèle. Visualisez les propriétés pour le modèle de création récente, et cliquez sur l'**onglet Sécurité**. Les autorisations décrivent quelle entité est permise pour demander un certificat qui utilise ce modèle, ainsi des autorisations correctes sont exigées. Dans cet exemple, l'entité est le service OCSP qui s'exécute sur le même hôte (TEST-CISCO \ C.C), et les besoins de service OCSP Autoenroll des privilèges :

   Toutes autres configurations pour le modèle peuvent être placées pour se transférer.

2. Lancez le modèle. Naviguez vers **CA > modèle de certificat > nouveau > modèle de certificat à émettre**, et pour sélectionner le modèle en double :

Certificat de service OCSP

Cette procédure décrit comment utiliser la gestion de la configuration en ligne afin de configurer OCSP :

1. Naviguez vers le **gestionnaire du serveur** > les **outils**.

2. Naviguez vers la **configuration de révocation > ajoutent la configuration de révocation** afin d'ajouter une nouvelle configuration :

   OCSP peut utiliser la même entreprise CA. Le certificat pour le service OCSP est généré.

3. Utilisez l'entreprise sélectionnée CA, et choisissez le modèle créé plus tôt. Le certificat est inscrit automatiquement :

4. Confirmez que le certificat est inscrit et son état est Working/OK :

5. Naviguez vers **CA >** les **Certificats délivrés** afin de vérifier les détails de certificat :

Nonces de service OCSP

L'implémentation de Microsoft d'OCSP est conforme avec RFC 5019 le profil en ligne léger de Protocol d'état de certificat (OCSP) pour les environnements à fort débit, qui est une version simplifiée d'état en ligne Protocol de certificat d'infrastructure de clé publique de l'Internet X.509 RFC 2560 - OCSP.

L'ASA utilise RFC 2560 pour OCSP. Une des différences dans les deux RFC est que RFC 5019 ne reçoit pas des demandes signées envoyées par ASA.

Il est possible de forcer le service de Microsoft OCSP à recevoir ces demandes signées et à répondre avec la réponse signée correcte. Naviguez vers la **configuration de révocation >** le **RevocationConfiguration1 > éditent Properties**, et sélectionnent l'option **d'activer le support d'extension de NONCE**.

Le service OCSP est maintenant prêt à employer.

Bien que Cisco ne recommande pas ceci, des nonces peuvent être désactivés sur l'ASA :

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

Configuration CA pour des extensions OCSP

Vous devez maintenant modifier le CA pour inclure l'extension de serveur OCSP dans tous les Certificats délivrés. L'URL de cette extension est utilisé par ASA afin de se connecter au serveur OCSP quand un certificat est validé.

1. Ouvrez la boîte de dialogue Properties pour le serveur sur le CA.

2. Cliquez sur l'onglet d'**extensions**. L'extension d'accès aux informations d'autorité (AIA) qui indique le service OCSP est nécessaire ; dans cet exemple, c'est http://10.61.208.243/ocsp. Activez chacun des deux options pour l'extension d'AIA :

   Incluez dans l'extension d'AIA des Certificats délivrésIncluez dans l'extension en ligne du protocole d'état de certificat (OCSP)

   Ceci s'assure que tous les Certificats délivrés ont une extension correcte ces points au service OCSP.

OpenSSL

> Remarque: Voir le guide de configuration de gamme de Cisco ASA 5500 utilisant le CLI, les 8.4 et les 8.6 : Configurer un serveur externe pour l'autorisation d'utilisateur de dispositifs de sécurité pour des détails sur la configuration de l'ASA par le CLI.

Cet exemple suppose que le serveur d'OpenSSL est déjà configuré. Cette section décrit seulement la configuration et les modifications OCSP qui sont nécessaires pour la configuration CA.

Cette procédure décrit comment générer le certificat OCSP :

1. Ces paramètres sont nécessaires pour le responder OCSP :

   ```
   BSNS-ASA5510-3(config-ca-trustpoint)# ocsp disable-nonce
   ```
2. Ces paramètres sont nécessaires pour des certificats utilisateurs :

   ```
   BSNS-ASA5510-3(config-ca-trustpoint)# ocsp disable-nonce
   ```
3. Des Certificats doivent être générés et signés par le CA.

4. Mettez en marche le serveur OCSP :

   ```
   BSNS-ASA5510-3(config-ca-trustpoint)# ocsp disable-nonce
   ```
5. Testez le certificat d'exemple :

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

Plus d'exemples sont disponibles sur le site Web d'OpenSSL.

OpenSSL, comme l'ASA, prend en charge des nonces OCSP ; les nonces peuvent être contrôlés avec l'utilisation - nonce et - des Commutateurs de no_nonce.

ASA avec de plusieurs sources OCSP

L'ASA peut ignorer l'OCSP URL. Même si le certificat client contient un OCSP URL, il est remplacé par la configuration sur l'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
```

L'adresse du serveur OCSP peut être définie explicitement. Cet exemple de commande apparie tous les Certificats avec l'administrateur dans le nom du sujet, emploie un point de confiance OPENSSL afin de valider la signature OCSP, et emploie l'URL de http://11.11.11.11/ocsp afin d'envoyer la demande :

```
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 commande utilisée pour trouver l'OCSP URL est :

1. Un serveur OCSP que vous avez placé avec la commande de **certificat de correspondance**
2. Un serveur OCSP que vous avez placé avec la commande d'**ocsp url**
3. Le serveur OCSP dans le domaine d'AIA du certificat client

ASA avec OCSP signé par CA différent

Une réponse OCSP peut être signée par un CA différent en pareil cas, il est nécessaire pour employer la commande de **certificat de correspondance** afin d'utiliser un point de confiance différent sur l'ASA pour la validation de certificat 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
```

Dans cet exemple, l'ASA utilise la réécriture d'OCSP URL pour tous les Certificats avec un subject-name qui contient l'administrateur. L'ASA est forcée pour valider le certificat de responder OCSP contre un autre point de confiance, OPENSSL. Des certificats utilisateurs sont encore validés dans le point de confiance WIN2012.

Puisque le certificat de responder OCSP a le « OCSP aucune révocation vérifiant » l'extension, le certificat n'est pas vérifié, même lorsqu'OCSP est forcé pour valider contre le point de confiance OPENSSL.

Par défaut, tous les points de confiance sont recherchés quand l'ASA essaye de vérifier le certificat utilisateur. La validation pour le certificat de responder OCSP est différente. L'ASA recherche seulement le point de confiance qui a été déjà trouvé pour le certificat utilisateur (WIN2012 dans cet exemple).

Ainsi, il est nécessaire d'employer la commande de **certificat de correspondance** afin de forcer l'ASA à utiliser un point de confiance différent pour la validation de certificat OCSP (OPENSSL

dans cet exemple).

Des certificats utilisateurs sont validés contre le premier point de confiance apparié (WIN2012 dans cet exemple), qui détermine alors le point de confiance par défaut pour la validation de responder OCSP.

Si aucun point de confiance spécifique n'est fourni dans la commande de **certificat de correspondance**, le certificat OCSP est validé contre le même point de confiance que les certificats utilisateurs (WIN2012 dans cet exemple). :

```
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
```

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

> Remarque: L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

ASA - Obtenez le certificat par l'intermédiaire de SCEP

Cette procédure décrit comment obtenir le certificat par l'utilisation de SCEP :

1. C'est la procédure d'authentification de point de confiance pour obtenir le certificat 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. Afin de demander le certificat, l'ASA doit avoir un mot de passe une fois SCEP qui peut être obtenu de la console d'admin chez http://IP/certsrv/mscep_admin :

3. Employez ce mot de passe pour demander le certificat sur l'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 certListUne certaine sortie a été omise pour la clarté.
```

4. Vérifiez les Certificats CA et 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
```

L'ASA n'affiche pas la plupart des extensions de certificat. Quoique le certificat ASA contienne « OCSP URL l'extension à AIA », l'ASA CLI ne la présente pas. ID de bogue Cisco CSCui44335, « extensions du certificat x509 ASA ENH affichées, » demande cette amélioration.

AnyConnect - Obtenez le certificat par l'intermédiaire de la page Web

Cette procédure décrit comment obtenir le certificat par l'utilisation du navigateur Web sur le client :

1. Un certificat utilisateur d'AnyConnect peut être demandé par la page Web. Sur le PC client, utilisez un navigateur Web pour s'attaquer au CA chez http:// *IP/certsrv* :

2. Le certificat utilisateur peut être enregistré dans la mémoire de navigateur Web, puis être exporté à Microsoft la mémoire, qui est recherchée par AnyConnect. Utilisation certmgr.msc afin de vérifier le certificat reçu :

   AnyConnect peut également demander le certificat tant que il y a un profil correct d'AnyConnect.

Accès à distance ASA VPN avec la validation OCSP

Cette procédure décrit comment vérifier la validation OCSP :

1. Comme il tente de se connecter, les états ASA que le certificat est OCSP vérifié. Ici, le certificat de signature OCSP a une extension de NO--contrôle et n'a pas été vérifié par l'intermédiaire d'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: 240000001B2AD208B12811687400000000001B, 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: 240000001B2AD208B12811687400000000001B, 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.
```

Une certaine sortie a été omise pour la clarté.

2. L'utilisateur final fournit les identifiants utilisateurs :

3. La session VPN est terminée correctement :

```
%ASA-7-717036: Looking for a tunnel group match based on certificate maps
for peer certificate with serial number:
240000001B2AD208B12811687400000000001B, 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: 240000001B2AD208B12811687400000000001B,
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. La session est créée :

```
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. Vous pouvez utiliser détaillé met au point pour la validation 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. Au niveau de capture de paquet, c'est la demande OCSP et la réponse correcte OCSP. La réponse inclut la signature correcte - extension de nonce activée sur Microsoft OCSP :

Accès à distance ASA VPN avec de plusieurs sources OCSP

Si un certificat de correspondance est configuré comme expliqué dans l'ASA avec de plusieurs sources OCSP, il a la priorité :

```
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
```

Quand un dépassement d'OCSP URL est utilisé, met au point sont :

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

Accès à distance ASA VPN avec OCSP et certificat retiré

Cette procédure décrit comment retirer le certificat et confirmer l'état retiré :

1. Retirez le certificat client :

2. Éditez les résultats :

3. Étapes [facultatives] 1 et 2 peuvent également être faites avec l'utilitaire CLI de certutil dans le shell d'alimentation :

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

4. Quand les essais de client à connecter, il y a une erreur de validation de certificat :

5. Les logs d'AnyConnect indiquent également l'erreur de validation de certificat :

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

6. L'ASA signale l'état de certificat est retirée :

```
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. Les captures de paquet affichent une réponse réussie OCSP avec l'état de certificat de retirer :

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Serveur OCSP vers le bas

L'ASA signale quand le serveur OCSP est en panne :

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

Les captures de paquet peuvent également aider avec le dépannage.

Temps non synchronisé

Si le temps en cours sur le serveur OCSP est plus ancien que sur l'ASA (les petites différences sont acceptables), le serveur OCSP envoie une réponse non autorisée, et l'ASA la signale :

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

Quand l'ASA reçoit une réponse OCSP de futures périodes, elle échoue également.

Nonces signés non pris en charge

Si des nonces sur le serveur ne sont pas pris en charge (qui est le par défaut sur Microsoft Windows 2012 R2), une réponse non autorisée est renvoyée :

Authentification de serveur IIS7

Les problèmes avec une demande SCEP/OCSP sont souvent le résultat de l'authentification incorrecte sur l'Internet Information Services 7 (IIS7). Assurez-vous que l'accès anonyme est configuré :

Informations connexes

- TechNet de Microsoft : Installation de responder, configuration, et guide de dépannage en ligne
- TechNet de Microsoft : Configurez un CA pour prendre en charge des responders OCSP
- Référence de commandes de gamme de Cisco ASA

- Support et documentation techniques - Cisco Systems