Acesso remoto VPN ASA com verificação OCSP sob Microsoft Windows 2012 e o OpenSSL

Índice

Introdução

Este documento descreve como usar a validação em linha do protocolo status do certificado (OCSP) em uma ferramenta de segurança adaptável de Cisco (ASA) para os Certificados apresentados por usuários VPN. Os exemplos de configuração para dois server OCSP ([CA] e OpenSSL do Certificate Authority de Microsoft Windows) são apresentados. A seção da

verificação descreve fluxos detalhados no nível do pacote, e a seção da pesquisa de defeitos centra-se sobre erros típicos e problemas.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do comando line interface(cli) da ferramenta de segurança de Cisco e configuração de VPN adaptáveis do Secure Socket Layer (SSL)
- Certificados X.509
- Microsoft Windows server
- Linux/OpenSSL

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Software adaptável da ferramenta de segurança de Cisco, versão 8.4 e mais recente
- Microsoft Windows 7 com Cliente de mobilidade Cisco AnyConnect Secure, liberação 3.1
- Servidor Microsoft 2012 R2
- Linux com OpenSSL 1.0.0j ou mais tarde

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

> Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

O cliente usa o acesso remoto VPN. Este acesso pode ser Cisco VPN Client (IPsec), mobilidade segura de Cisco AnyConnect (versão 2 [IKEv2] das trocas de chave SSL/Internet), ou WebVPN (portal). A fim entrar, o cliente fornece o certificado correto, assim como o username/senha que foi configurada localmente no ASA. O certificado de cliente é validado através do server OCSP.

Acesso remoto ASA com OCSP

O ASA é configurado para o acesso SSL. O cliente está usando AnyConnect a fim entrar. O ASA

usa o protocolo simple certificate enrollment (SCEP) a fim pedir o 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
```

Um mapa do certificado é criado a fim identificar todos os usuários cujo o assunto-nome contém o administrador da palavra (não diferenciando maiúsculas e minúsculas). Aqueles usuários são limitados a um grupo de túneis nomeado 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
```

A configuração de VPN exige a autorização bem sucedida (isto é, um certificado validado). Igualmente exige as credenciais corretas para o username localmente definido (autenticação 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: Veja o manual de configuração do 5500 Series de Cisco ASA usando o CLI, os 8.4 e os 8.6: Configurando um servidor interno para a autorização de usuário da ferramenta de segurança para detalhes na configuração do ASA com o CLI.

A instalação dos serviços

Este procedimento descreve como configurar serviços do papel para o servidor Microsoft:

1. Navegue ao **gerenciador do servidor > controlam papéis e características do** > Add. O servidor Microsoft precisa estes serviços do papel:

Autoridade de certificaçãoRegistro da Web da autoridade de certificação, que é usado pelo clienteQue responde em linha, que é precisado para OCSPO serviço do registro do dispositivo de rede, que contém o aplicativo SCEP usou-se pelo ASA O serviço de Web com políticas pode ser adicionado se necessário.

2.
3.
4. Quando você adiciona características, seja certo incluir ferramentas em linha do que responde porque inclui um OCSP pressão-naquele é usado mais tarde:

Configuração de CA para o molde OCSP

O serviço OCSP usa um certificado para assinar a resposta OCSP. Um certificado especial no servidor Microsoft deve ser gerado e deve incluir:

- Uso chave prolongado = assinatura OCSP
- OCSP nenhuma verificação da revogação

Este certificado é precisado a fim impedir laços da validação OCSP. O ASA não usa o serviço OCSP para tentar verificar o certificado apresentado pelo serviço OCSP.

1. Adicionar um molde para o certificado no CA navegam a **CA >** ao **molde de certificado > controlam**, **resposta** seleta **OCSP que assina**, e duplicam o molde. Veja as propriedades para o molde recém-criado, e clique a **ABA de segurança**. As permissões descrevem que entidade é permitida pedir um certificado que use esse molde, assim que as permissões correta são exigidas. Neste exemplo, a entidade é o serviço OCSP que está sendo executado no mesmo host (TEST-CISCO \ DC), e as necessidades do serviço OCSP Autoenroll privilégios:

   Todos ajustes restantes para o molde podem ser ajustados para optar.

2. Ative o molde. Navegue a **CA >** ao **molde de certificado > novo > molde de certificado a emitir**, e selecionar o molde duplicado:

Certificado do serviço OCSP

Este procedimento descreve como usar o Gerenciamento de configuração online a fim configurar OCSP:

1. Navegue ao **gerenciador do servidor >** às **ferramentas**.

2. Navegue à **configuração da revogação do >** Add da **configuração da revogação** a fim adicionar uma configuração nova:

OCSP pode usar a mesma empresa CA. O certificado para o serviço OCSP é gerado.

3. Use a empresa selecionada CA, e escolha o molde criado mais cedo. O certificado é registrado automaticamente:

4. Confirme que o certificado está registrado e seu estado é Working/OK:

5. Navegue a **CA > Certificados emitidos** a fim verificar os detalhes certificados:

Nonces do serviço OCSP

A aplicação de Microsoft de OCSP é complacente com RFC 5019 o perfil em linha de pouco peso do protocolo status do certificado (OCSP) para ambientes do volume alto, que é uma versão simplificada do protocolo status em linha do certificado da infraestrutura de chave pública do Internet do RFC 2560 X.509 - OCSP.

O ASA usa o RFC 2560 para OCSP. Uma das diferenças nos dois RFC é que o RFC 5019 não aceita os pedidos assinados enviados pelo ASA.

Épossível forçar o serviço de Microsoft OCSP para aceitar aqueles pedidos assinados e para responder com a resposta assinada correta. Navegue à **configuração da revogação >** ao **RevocationConfiguration1 > Edit Properties**, e selecione a opção **para permitir o apoio da extensão do NONCE**.

O serviço OCSP é agora pronto para uso.

Embora Cisco não recomende este, os nonces podem ser desabilitados no ASA:

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

Configuração de CA para Ramais OCSP

Você deve agora reconfigurar CA para incluir a extensão de servidor OCSP em todos os Certificados emitidos. A URL dessa extensão está usada pelo ASA a fim conectar ao server OCSP quando um certificado é validado.

1. Abra a caixa de diálogo das propriedades para o server em CA.

2. Clique a aba dos **Ramais**. A extensão do acesso à informação da autoridade (AIA) que aponta ao serviço OCSP é precisada; neste exemplo, é http://10.61.208.243/ocsp. Permita both of these opções para a extensão de AIA:

Inclua na extensão de AIA de Certificados emitidosInclua na extensão em linha do protocolo status do certificado (OCSP)

Isto assegura-se de que todos os Certificados emitidos tenham uma extensão correta esses pontos ao serviço OCSP.

OpenSSL

Nota: Veja o manual de configuração do 5500 Series de Cisco ASA usando o CLI, os 8.4 e os 8.6: Configurando um servidor interno para a autorização de usuário da ferramenta de segurança para detalhes na configuração do ASA com o CLI.

Este exemplo supõe que o server do OpenSSL está configurado já. Esta seção descreve somente a configuração e as mudanças OCSP que são precisadas para a configuração de CA.

Este procedimento descreve como gerar o certificado OCSP:

1. Estes parâmetros são precisados para o que responde OCSP:

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

2. Estes parâmetros são precisados para certificados de usuário:

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

3. Os Certificados precisam de ser gerados e assinado por CA.

4. Ligue o server OCSP:

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

5. Teste o certificado do exemplo:

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

Mais exemplos estão disponíveis no site do OpenSSL.

O OpenSSL, como o ASA, apoia nonces OCSP; os nonces podem ser controlados com uso -nonce e - do Switches do no_nonce.

ASA com fontes múltiplas OCSP

O ASA pode cancelar o OCSP URL. Mesmo se o certificado de cliente contém um OCSP URL, overwritten pela configuração no 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
```

O endereço do servidor OCSP pode ser definido explicitamente. Este comando example combina todos os Certificados com o administrador no nome do sujeito, usa um ponto confiável do

OPENSSL a fim validar a assinatura OCSP, e usa a URL de http://11.11.11.11/ocsp a fim enviar o pedido:

```
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
```

A ordem usada para encontrar OCSP URL é:

1. Um server que OCSP você se ajustou com o **comando certificate do fósforo**
2. Um server que OCSP você se ajustou com o **comando url do ocsp**
3. O server OCSP no campo de AIA do certificado de cliente

ASA com o OCSP assinado por CA diferente

Uma resposta OCSP pode ser assinada por CA diferente. Em tal caso, é necessário usar o **comando certificate do fósforo** a fim usar um ponto confiável diferente no ASA para a validação certificada 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
```

Neste exemplo, o ASA usa a reescrita OCSP URL para todos os Certificados com um assunto-nome que contenha o administrador. O ASA é forçado a validar o certificado do que responde OCSP contra um outro ponto confiável, OPENSSL. Os certificados de usuário são validados ainda no ponto confiável WIN2012.

Desde que o certificado do que responde OCSP tem o “OCSP nenhuma revogação que verifica” a extensão, o certificado não está verificado, mesmo quando OCSP é forçado a validar contra o ponto confiável do OPENSSL.

Àrevelia, todos os pontos confiáveis são procurados quando o ASA está tentando verificar o certificado de usuário. A validação para o certificado do que responde OCSP é diferente. O ASA procura somente o ponto confiável que tem sido encontrado já para o certificado de usuário (WIN2012 neste exemplo).

Assim, é necessário usar o **comando certificate do fósforo** a fim forçar o ASA para usar um ponto confiável diferente para a validação certificada OCSP (OPENSSL neste exemplo).

Os certificados de usuário são validados contra o primeiro ponto confiável combinado (WIN2012 neste exemplo), que determina então o ponto confiável do padrão para a validação do que responde OCSP.

Se nenhum ponto confiável específico é fornecido no **comando certificate do fósforo**, o certificado OCSP está validado contra o mesmo ponto confiável que os certificados de usuário (WIN2012 neste exemplo).:

```
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
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

> Nota: A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

ASA - Obtenha o certificado através do SCEP

Este procedimento descreve como obter o certificado com o uso do SCEP:

1. Este é o processo de autenticação do ponto confiável para obter o 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. A fim pedir o certificado, o ASA precisa de ter uma único senha SCEP que possa ser obtida do console admin em http://IP/certsrv/mscep_admin:

3. Use essa senha para pedir o certificado no 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
```

Alguma saída foi omitida para maior clareza.

4. Verifique os Certificados de CA e 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
```

O ASA não indica a maioria das extensões de certificado. Mesmo que o certificado ASA contenha “OCSP URL a extensão em AIA”, o ASA CLI não a apresenta. Identificação de bug Cisco CSCui44335, “Ramais do certificado x509 ASA ENH indicados,” pede este realce.

AnyConnect - Obtenha o certificado através do página da web

Este procedimento descreve como obter o certificado com o uso do navegador da Web no cliente:

1. Um certificado de usuário de AnyConnect pode ser pedido com o Web page. No PC cliente, use um navegador da Web para ir a CA em http:// *IP/certsrv*:

2. O certificado de usuário pode ser salvar na loja do navegador da Web, a seguir ser para Microsoft a loja, que procurada por AnyConnect. Use certmgr.msc a fim verificar o certificado recebido:

   AnyConnect pode igualmente pedir o certificado enquanto há um perfil correto de AnyConnect.

Acesso remoto ASA VPN com validação OCSP

Este procedimento descreve como verificar a validação OCSP:

1. Enquanto tenta conectar, o ASA relata que o certificado está sendo verificado para ver se há OCSP. Aqui, o certificado de assinatura OCSP tem uma extensão da nenhum-verificação e não foi verificado através 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: 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.
```

Alguma saída foi omitida para maior clareza.

2. O utilizador final fornece as credenciais do usuário:

3. A sessão de VPN é terminada corretamente:

```
%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. A sessão é criada:

```
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. Você pode usar detalhado debuga para a validação 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. A nível da captura de pacote de informação, esta é o pedido OCSP e a resposta correta OCSP. A resposta inclui a assinatura correta - extensão do nonce permitida em Microsoft OCSP:

Acesso remoto ASA VPN com fontes múltiplas OCSP

Se um certificado do fósforo é configurado como explicado no ASA com fontes múltiplas OCSP, toma a precedência:

```
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
```

Quando uma ultrapassagem OCSP URL é usada, debuga são:

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

Acesso remoto ASA VPN com OCSP e o certificado revogado

Este procedimento descreve como revogar o certificado e confirmar o estado revogado:

1. Revogue o certificado de cliente:

2. Publique os resultados:

3. Etapas 1 e 2 do [Optional] podem igualmente ser executadas com o utilitário de CLI do certutil no shell da potência:

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

4. Quando o cliente tenta conectar, há um erro da validação certificada:

5. Os logs de AnyConnect igualmente indicam o erro da validação certificada:

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

6. O ASA relata que o estado do certificado está revogado:

```
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. As capturas de pacote de informação mostram uma resposta bem sucedida OCSP com o estado do certificado do revogado:

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Server OCSP para baixo

O ASA relata quando o server OCSP está para baixo:

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

As capturas de pacote de informação podem igualmente ajudar com Troubleshooting.

Tempo não sincronizado

Se as horas atual no server OCSP são mais velhas do que no ASA (as diferenças pequenas são aceitáveis), o server OCSP envia uma resposta desautorizada, e o ASA relata-a:

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

Quando o ASA recebe uma resposta OCSP das épocas futuras, igualmente falha.

Nonces assinados não apoiados

Se os nonces no server não estão apoiados (que é o padrão em Microsoft Windows 2012 R2), uma resposta desautorizada está retornada:

Autenticação de servidor IIS7

Os problemas com um pedido SCEP/OCSP são frequentemente o resultado da autenticação incorreta no Internet Information Services 7 (IIS7). Assegure-se de que o acesso anônimo esteja configurado:

Informações Relacionadas

- Microsoft TechNet: A instalação, configuração, e guia de Troubleshooting em linha do que responde
- Microsoft TechNet: Configurar CA para apoiar que respondes OCSP
- Referência de comandos da série de Cisco ASA
- Suporte Técnico e Documentação - Cisco Systems