

Problembehandlung bei der Zertifikatsperrliste für die Authentifizierung über AnyConnect-Zertifikate

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Topologie](#)

[Wichtige Konfiguration](#)

[CA-Router](#)

[Konfiguration des VPN-Gateways](#)

[Windows-Gerät](#)

[Validierung](#)

[Szenario 1. Das Zertifikat ist für die Authentifizierung gültig.](#)

[Szenario 2. Das Zertifikat wird widerrufen, und die Authentifizierung schlägt fehl.](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird die Fehlerbehebung für die Zertifikatsperrliste (Certificate Revocation List, CRL) beschrieben, die für die zertifikatbasierte AnyConnect-Authentifizierung konfiguriert wurde.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Zertifizierungsstelle
- Public Key Infrastructure (PKI)
- RA VPN auf FTD
- Windows 10 mit AnyConnect-Client

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

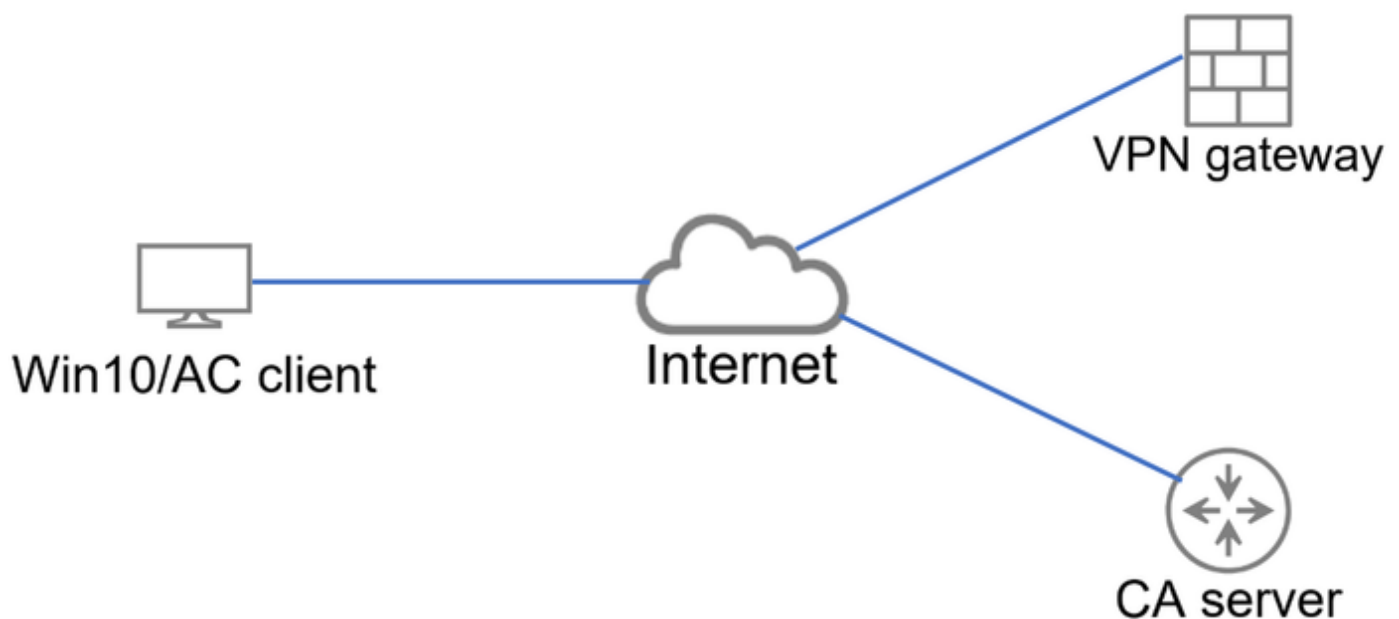
- CSR1000V - Cisco IOS® XE, Version 16.12.03 - als Cisco IOS XE CA-Server
- NGFWv - Version 7.1.0 - als VPN-Gateway
- AnyConnect Secure Mobility Client Version 4.10.07073 - als VPN-Client
- Windows 10 als lokaler Computer

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Mit der Zertifikatsperrliste können Geräte feststellen, ob ein Zertifikat vor Ablauf der Lebensdauer des Zertifikats widerrufen wurde. Eine Zertifikatsperrliste enthält die Seriennummer und das Widerrufsdatum des Zertifikats. Ein sicheres Gateway wie FirePOWER Thread Defense (FTD)-Systeme oder andere Endgeräte nutzt diese Funktion, um die Zertifikatsauthentifizierung durch Validierung des Zertifikatsstatus zu stärken.

Topologie



Grundlegende Topologie, die Verbindungen zum VPN-Gateway und zum CA-Server bereitstellt.

Wichtige Konfiguration

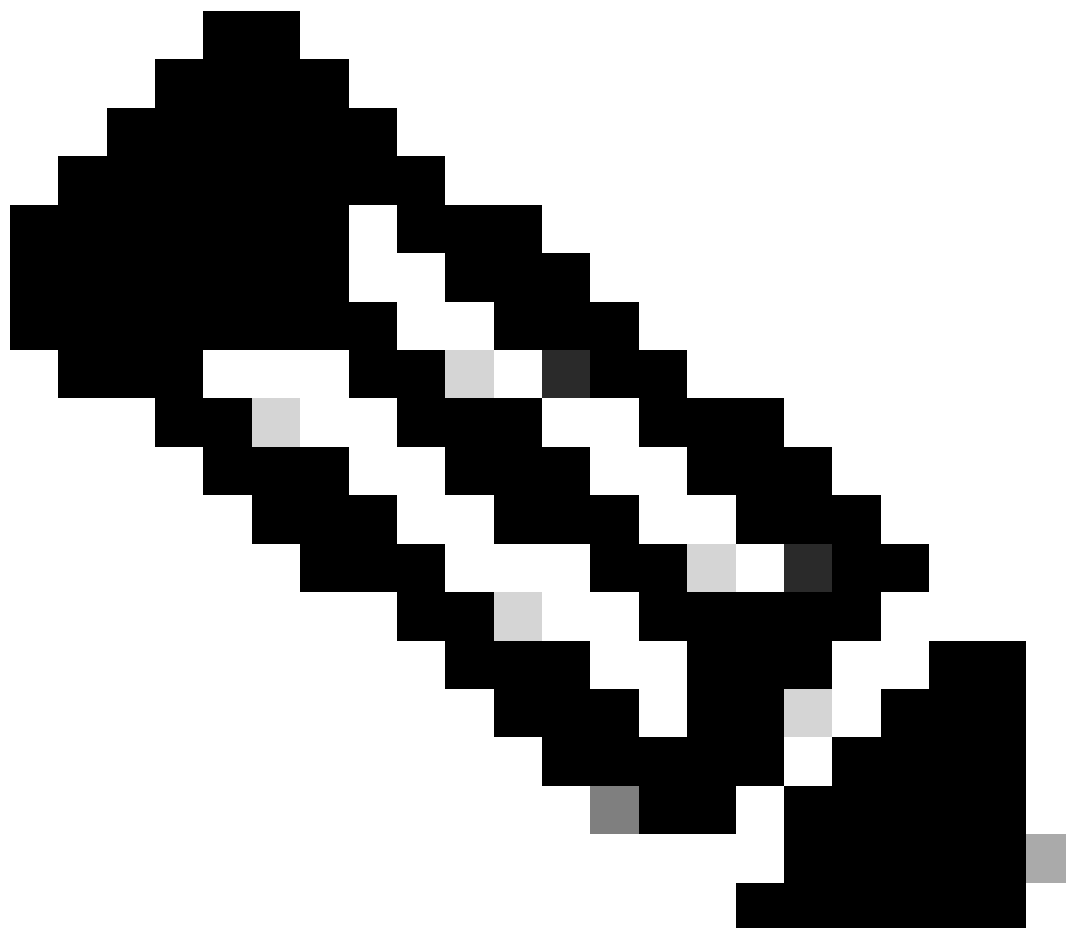
Um eine zertifikatbasierte Authentifizierung mit der Zertifikatsperrliste zu erreichen, wurde die dargestellte Konfiguration auf allen beteiligten Geräten verwendet.

CA-Router

Die Serverzertifizierungsstelle ist für die Ausstellung von Identitätszertifikaten für die Benutzer

zuständig, um die Authentifizierung für das VPN-Gateway bereitzustellen. Darüber hinaus speichert der Router die CRL-Datenbankdatei und fungiert als CRL Distribution Point (CDP).

Bei einem CDP rufen das VPN-Gateway und andere Endbenutzer die CRL-Informationen ab. Diese Informationen werden lokal zwischengespeichert und sind nur für einen bestimmten Zeitraum gültig. Wenn diese Zeit abläuft, wird eine neue Zertifikatsperrliste heruntergeladen.



Hinweis: Die Zertifikatsperrlisten-Datenbank und der Standort, an dem die Geräte Zugriff auf die Zertifikatsperrliste haben, können sich auf demselben Gerät befinden. Aus Sicherheitsgründen wird jedoch empfohlen, das Zertifikatsperrlisten, auf das Endgeräte zugreifen, in einem anderen Gerät als der Zertifikatsperrlisten-Datenbank zu speichern. In diesem Beispiel speichert der CA-Router die CRL-Datenbank und fungiert als CDP für das VPN-Gateway.

<#root>

crypto pki server CAS

```

database level complete
no database archive
issuer-name cn=calo_root,ou=TAC,o=cisco
grant auto
hash sha256

lifetime crl 2

lifetime certificate 300
lifetime ca-certificate 1000

cdp-url http://192.0.2.10/cgi-bin/pkiclient.exe?operation=GetCRL

eku server-auth client-auth
database url ser nvram:

crypto pki trustpoint TP-self-signed-1507329386
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-1507329386
revocation-check none
rsakeypair TP-self-signed-1507329386

crypto pki trustpoint CAS
revocation-check crl
rsakeypair CAS

interface GigabitEthernet2
ip address 192.0.2.10 255.255.255.0
negotiation auto

ip http server

ntp master 1

```

Konfiguration des VPN-Gateways

Das FTD wird so konfiguriert, dass Endbenutzern ein Remote Access VPN bereitgestellt wird, das Zertifikate als Authentifizierungsmethode verwendet (nur Zertifikat). Nach Erhalt des Identitätszertifikats vom Benutzer überprüft der FTD, ob das Zertifikat von einer bekannten Zertifizierungsstelle (Certificate Authority, CA) ausgestellt wurde, und bestätigt seine Gültigkeit, indem er die Zertifikatsperrliste aus dem im Zertifikat definierten CDP bezieht.

```

<#root>

tunnel-group local type remote-access
tunnel-group local general-attributes
address-pool AC_pool
default-group-policy local_gp
username-from-certificate use-entire-name
tunnel-group local_test webvpn-attributes

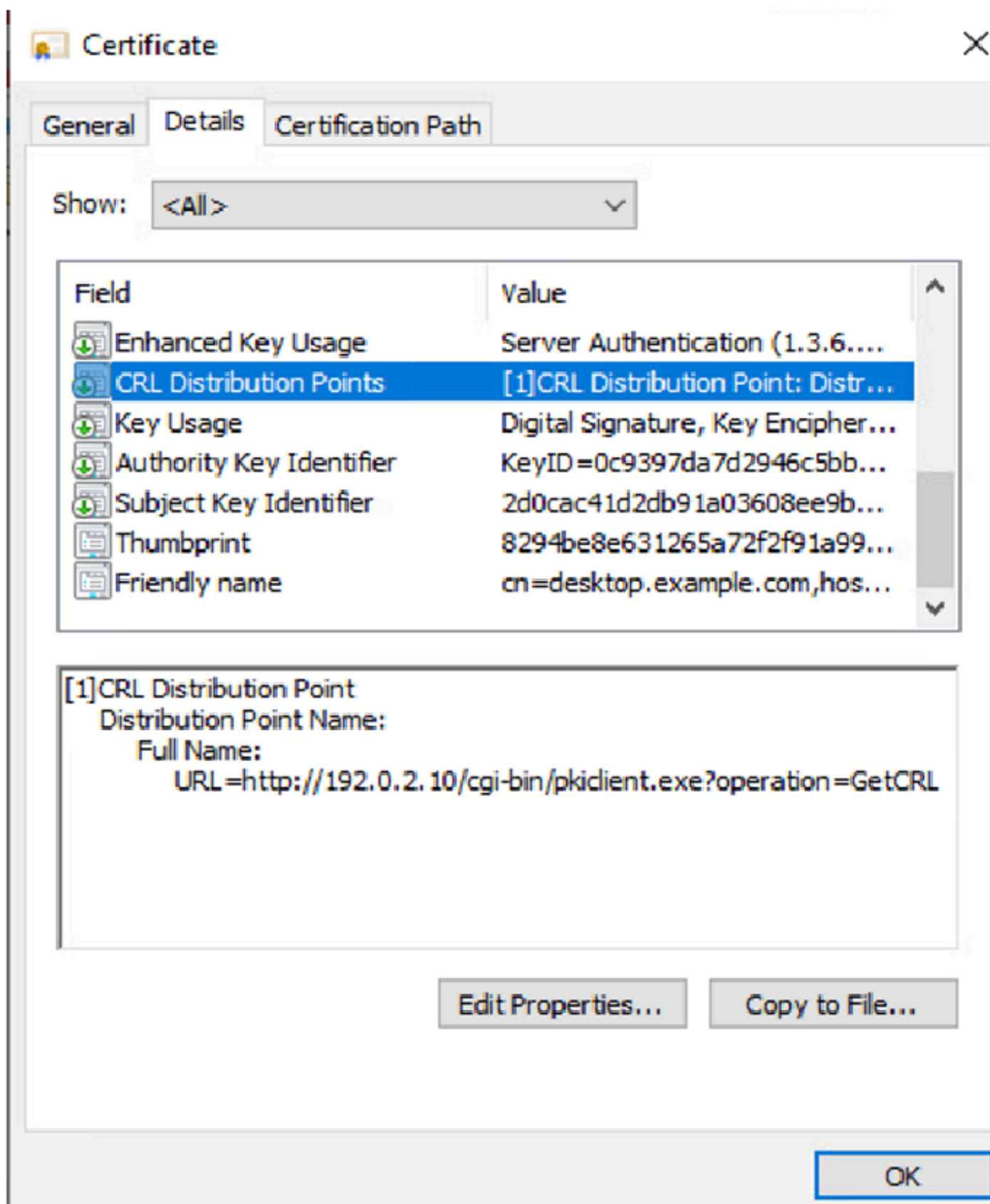
authentication certificate

group-alias test enable

```

Windows-Gerät

Ein Identitätszertifikat wurde vom Zertifizierungsstellenserver ausgestellt und auf dem Windows-Gerät installiert.



Validierung

Die nächsten Debugs und Erfassungen zeigen den Unterschied zwischen einem Benutzer mit einem gültigen Zertifikat (Arbeitsszenario) und einem Benutzer mit einem Zertifikat, das widerrufen wurde (Arbeitsszenario).

Szenario 1. Das Zertifikat ist für die Authentifizierung gültig.

Wenn der Benutzer den Verbindungsversuch startet, stellt er dem FTD sein Identitätszertifikat zur Verfügung, das VPN-Gateway verifiziert, dass es sich bei dem Aussteller um eine bekannte Behörde handelt, und fordert die CRL über eine HTTP/GET-Anforderung von dem im Identitätszertifikat definierten CDP an. Der CA-Server antwortet mit der Zertifikatsperrliste, und die FTD prüft, ob die Seriennummer des Zertifikats aufgeführt ist. Da die Zertifikatsperrliste leer ist (keine gesperrten Zertifikate), akzeptiert die FTD das Zertifikat als gültig und ermöglicht dem Benutzer die Authentifizierung.

<#root>

```
PKI[7]: Cert to verify
PKI[7]: -----Certificate-----:
Serial Number: 2 (0x2)
Issuer: O=cisco, OU=TAC, CN=calo_root
Subject: CN=desktop.example.com/unstructuredName=CA-router

PKI[12]: pki_verify_cb, pki_oss1_validate.c:358
PKI[8]: val status=1: cert subject: /O=cisco/OU=TAC/CN=calo_root. ctx->error: (0)ok, cert_idx: 1
PKI[12]: pki_verify_cb, pki_oss1_validate.c:358
PKI[8]: val status=1: cert subject: /CN=desktop.example.com/unstructuredName=CA-router. ctx->error: (0)
PKI[8]: pki_oss1_find_valid_chain took 217 microsecs
PKI[6]: Verified chain:
PKI[14]: pki_oss1_get_cert_summary, pki_oss1.c:119
PKI[6]: -----Certificate-----:
Serial Number: 2 (0x2)
Issuer: O=cisco, OU=TAC, CN=calo_root
Subject: CN=desktop.example.com/unstructuredName=CA-router

PKI[14]: pki_oss1_get_cert_summary, pki_oss1.c:119
PKI[6]: -----Certificate-----:
Serial Number: 1 (0x1)
Issuer: O=cisco, OU=TAC, CN=calo_root
Subject: O=cisco, OU=TAC, CN=calo_root
```

[..output ommitted]

```
CRYPTO_PKI: bitValue of KEY_USAGE = a0PKI[7]: CRYPTO_PKI:check_key_usage: Checking KU for case VPN peer
PKI[7]: CRYPTO_PKI:check_key_usage: KU bit digitalSignature is ON.
PKI[7]: ExtendedKeyUsage OID = serverAuth NOT acceptable for usage type SSL VPN Peer
PKI[7]: ExtendedKeyUsage OID = clientAuth acceptable for usage type: SSL VPN Peer
PKI[7]: check_key_usage:Extended Key/Key Usage check OK
PKI[12]: pki_oss1_revocation_check, pki_oss1_validate.c:931
PKI[7]: Starting revocation check for session 0x06c8d45f
PKI[12]: pki_init_revocation, pki_oss1_revocation.c:162
PKI[12]: pki_oss1_eval_revocation, pki_oss1_validate.c:699
PKI[7]: Evaluating session revocation status, 1 certs to check
```

PKI[8]: session 0x06c8d45f, cert 0 has rev_status 0, using methods 1/3/0 at index 0
PKI[12]: cert_revoc_exempt, pki_ossl_revocation.c:250
PKI[13]: get_tp_from_policy, pki_ossl_policy_transition.c:230
PKI[11]: polinfo->name: CRL-AC
PKI[11]: tp label: Trustpool
PKI[13]: label: CRL-AC
PKI[13]: pki_crl_cached, pki_ossl_crl_cache.c:1351
PKI[13]: get_tp_from_policy, pki_ossl_policy_transition.c:230
PKI[11]: polinfo->name: CRL-AC
PKI[11]: tp label: Trustpool
PKI[13]: label: CRL-AC
PKI[12]: pki_ossl_check_cache, pki_ossl_crl_cache.c:1269
PKI[7]: Starting OSSL CRL cache check.
PKI[12]: pki_ossl_crypto_build_crdp_list, pki_ossl_crl_cache.c:326
PKI[12]: pki_get_der_cdp_ext, crypto_pki.c:1528
PKI[14]: url_type_allowed, pki_ossl_crl_cache.c:153

PKI[9]: Attempting to find cached CRL for CDP <http://192.0.2.10/cgi-bin/pkiclient.exe?operation=GetCRL>

PKI[12]: pki_ossl_SelectCRLByIssuerTimeDER, pki_ossl_crl_cache.c:1219
PKI[14]: pki_ossl_get_name_string, pki_ossl.c:315
PKI[9]: Select DER crl(O=cisco, OU=TAC, CN=calo_root)
PKI[12]: pki_ossl_get_crl_internal, pki_ossl_crl_cache.c:506
PKI[7]: CRL not cached. Initiating CRL download for cert idx 0.
PKI[12]: do_get_crl, pki_ossl_revocation.c:85
PKI[9]: starting CRL FSM #0
PKI[11]: drive_fsm, pki_ossl_revocation.c:33
PKI[8]: [Sess: 0x06c8d45f, Cert: 0] FSM: In PKICRL_InitTransaction
PKI[12]: get_cdps, pki_crl_fsm_act.c:202
PKI[13]: get_tp_from_policy, pki_ossl_policy_transition.c:230
PKI[11]: polinfo->name: CRL-AC
PKI[11]: tp label: Trustpool
PKI[13]: label: CRL-AC
PKI[12]: pki_ossl_crypto_build_crdp_list, pki_ossl_crl_cache.c:326
PKI[12]: pki_get_der_cdp_ext, crypto_pki.c:1528
PKI[14]: url_type_allowed, pki_ossl_crl_cache.c:153

PKI[7]: cdp: (len=58, type=URI, prot=HTTP) <http://192.0.2.10/cgi-bin/pkiclient.exe?operation=GetCRL>

PKI[8]: [Sess: 0x06c8d45f, Cert: 0] FSM: PKICRL_InitTransaction, Return status: 0
PKI[8]: [Sess: 0x06c8d45f, Cert: 0] FSM: In PKICRL_NextCDP
PKI[12]: crldp_cdp_blacklisted, pki_ossl_crl.c:1374
PKI[12]: crl_find_pending_crl, pki_ossl_crl.c:1155
PKI[13]: get_pending_crl_list, pki_ossl_crl.c:1101
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:42
PKI[14]: cmp_cdp_info, pki_ossl_crl.c:1121
PKI[14]: cmp_cdp_info, pki_ossl_crl.c:1121
PKI[14]: cmp_cdp_info, pki_ossl_crl.c:1121
PKI[7]: CDP is not blacklisted
PKI[8]: [Sess: 0x06c8d45f, Cert: 0] FSM: PKICRL_NextCDP, Return status: 0
PKI[8]: [Sess: 0x06c8d45f, Cert: 0] FSM: In PKICRL_Request
PKI[13]: crldp_download_pending, pki_ossl_crl.c:1184
PKI[12]: crl_find_pending_crl, pki_ossl_crl.c:1155
PKI[13]: get_pending_crl_list, pki_ossl_crl.c:1101
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:42
PKI[14]: cmp_cdp_info, pki_ossl_crl.c:1121
PKI[14]: cmp_cdp_info, pki_ossl_crl.c:1121
PKI[14]: cmp_cdp_info, pki_ossl_crl.c:1121
PKI[8]: session 0x06c8d45f adding pending CRL entry for cert 0
PKI[12]: crldp_add_pending_download, pki_ossl_crl.c:1203
PKI[12]: crl_find_pending_crl, pki_ossl_crl.c:1155

```
PKI[13]: get_pending_crl_list, pki_oss1_crl.c:1101
PKI[13]: crypto_pki_get_oss1_env, pki_oss1.c:42
PKI[14]: cmp_cdp_info, pki_oss1_crl.c:1121
PKI[14]: cmp_cdp_info, pki_oss1_crl.c:1121
PKI[14]: cmp_cdp_info, pki_oss1_crl.c:1121
PKI[13]: get_pending_crl_list, pki_oss1_crl.c:1101
PKI[13]: crypto_pki_get_oss1_env, pki_oss1.c:42
PKI[12]: retrieve_crl, pki_crl_fsm_act.c:233
PKI[13]: get_tp_from_policy, pki_oss1_policy_transition.c:230
PKI[11]: polinfo->name: CRL-AC
PKI[11]: tp label: Trustpool
PKI[13]: label: CRL-AC
PKI[7]: CDP type HTTP

PKI[7]: getting http://192.0.2.10/cgi-bin/pkiclient.exe?operation=GetCRL

PKI[12]: pki_oss1_crl_build_http_io, pki_oss1_crl.c:1017
PKI[13]: pki_parse_uri, pki_oss1_uri.c:75
PKI[14]: pki_uri_map_protocol, pki_oss1_uri.c:17
PKI[14]: pki_uri_get_port, pki_oss1_uri.c:34
PKI[13]: pki_free_uri, pki_oss1_uri.c:57
PKI[11]: pki_crl_request_send_async, pki_oss1_crl.c:627
PKI[8]: [15] IOCB allocated
PKI[7]: PKI CRL I/O request queue result: IO_STATUS_QUEUED
PKI[8]: [Sess: 0x06c8d45f, Cert: 0] FSM: PKICRL_Request, Return status: 0
PKI[7]: Chain revocation status: good: 0, exempt: 0, cached: 0, revoked: 0, error: 0, pending: 1, fail-
PKI[9]: Async unlocked for session 0x06c8d45f
PKI[8]: [15] Received IO request msg

PKI[8]: [15] DNS resolve issued for 192.0.2.10

PKI[9]: CERT API thread sleeps!

PKI[7]: [15] DNS resolve 192.0.2.10 (192.0.2.10)

PKI[8]: [15] Socket open success

PKI[8]: [15] IPv4 Route lookup to 192.0.2.10 use interface outside

PKI[8]: [15] Connect sent to 192.0.2.10 from 192.0.2.1

PKI[12]: pki_io_cbfunc_log_revocation_check, pki_oss1_revocation.c:421
PKI[7]: 6717056: Attempting CRL revocation check from outside:192.0.2.1/62075 to 192.0.2.10/80 using HT

PKI[8]: [15] Received Socket transmit ready msg

----- Begin Data Type:HTTP Request [15]
Length: 76 -----
47 45 54 20 2f 63 67 69 2d 62 69 6e 2f 70 6b 69 | GET /cgi-bin/pki
63 6c 69 65 6e 74 2e 65 78 65 3f 6f 70 65 72 61 | client.exe?opera
74 69 6f 6e 3d 47 65 74 43 52 4c 20 48 54 54 50 | tion=GetCRL HTTP
2f 31 2e 30 0d 0a 48 6f192.0.2.10 73 74 3a 20 31 39 32 2e | /1.0..Host: 192.
31 38 31 2e 33 2e 31 30 0d 0a 0d 0a | 0.2.10....
----- End Data Type:HTTP Request [15]
Length: 76 -----
```


PKI[8]: [15] Sent 76 bytes
PKI[8]: [15] Received Socket read ready msg
PKI[8]: [15] read 662 bytes
PKI[8]: [15] Read EOF
PKI[12]: pki_io_cbfunc, pki_crl_fsm_act.c:59
PKI[7]: Callback received for vcid: 0, sess_id: 0x06c8d45f, cert_idx: 0, status: IO_STATUS_OK(1), data1
PKI[13]: get_fsm_data, pki_ossl_revocation.c:446
PKI[7]: [15] IOCB freed
PKI[13]: CERT_API_QueueFSMEvent, vpn3k_cert_api.c:137
PKI[13]: CERT_API_req_enqueue, vpn3k_cert_api.c:2913
PKI[9]: CERT API thread wakes up!
PKI[12]: CERT_API_Q_Process, vpn3k_cert_api.c:2811
PKI[12]: CERT_API_process_req_msg, vpn3k_cert_api.c:2746
PKI[8]: process msg cmd=2, session=0x06c8d45f
PKI[9]: Async locked for session 0x06c8d45f
PKI[11]: pki_notify_fsm_evt, pki_ossl_revocation.c:56
PKI[11]: drive_fsm, pki_ossl_revocation.c:33
PKI[8]: [Sess: 0x06c8d45f, Cert: 0] FSM: In PKICRL_ProcessResp
PKI[13]: pki_ossl_util_find_http_payload, pki_ossl_utils.c:36

PKI[8]: Received CRL of length 249 for session 0x06c8d45f, cert idx 0

PKI[13]: get_tp_from_policy, pki_ossl_policy_transition.c:230
PKI[11]: polinfo->name: CRL-AC
PKI[11]: tp label: Trustpool
PKI[13]: label: CRL-AC
PKI[12]: pki_ossl_crl_add_to_cache, pki_ossl_crl_cache.c:1177
PKI[12]: pki_ossl_crypto_verify_and_insert_crl, pki_ossl_crl_cache.c:1126
PKI[12]: pki_ossl_insert_der_crl_int, pki_ossl_crl_cache.c:1017
PKI[8]: Inserting CRL
PKI[14]: pki_ossl_get_crl_summary, pki_ossl.c:151
PKI[8]: -----CRL-----:
Certificate Revocation List (CRL):
Version 1 (0x0)
Signature Algorithm: sha1WithRSAEncryption
Issuer: /O=cisco/OU=TAC/CN=calo_root

Last Update: Sep 24 22:18:38 2023 GMT

Next Update: Sep 25 00:18:38 2023 GMT

No Revoked Certificates.

[..outout ommitted]

PKI[7]: Evaluating session revocation status, 1 certs to check

PKI[8]: session 0x06c8d45f, cert 0 has rev_status 3, using methods 1/3/0 at index 0
PKI[7]: Chain revocation status: good: 0, exempt: 0, cached: 1, revoked: 0, error: 0, pending: 0, fail-
PKI[7]: session: 0x06c8d45f, all revocation processing complete
PKI[5]: session: 0x06c8d45f, CRL for certificate 0 has been cached
PKI[12]: pki_ossl_rebuild_ca_store, pki_ossl_certstore.c:194
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:42
PKI[12]: pki_ossl_crl_add_cache_to_store, pki_ossl_crl_cache.c:1396
PKI[9]: OSSL certstore updated with 0 certs, 1 CRLs and 0 policies, 0 certs added to stack

PKI[7]: session 0x06c8d45f, Starting chain validation with cached CRL checking

PKI[12]: pki_ossl_find_valid_chain, pki_ossl_validate.c:472

PKI[9]: Begin sorted cert chain

PKI[14]: pki_ossl_get_cert_summary, pki_ossl.c:119

PKI[9]: -----Certificate-----:

Serial Number: 1 (0x1)

Issuer: O=cisco, OU=TAC, CN=calo_root

Subject: O=cisco, OU=TAC, CN=calo_root

PKI[14]: pki_ossl_get_cert_summary, pki_ossl.c:119

PKI[9]: -----Certificate-----:

Serial Number: 2 (0x2)

Issuer: O=cisco, OU=TAC, CN=calo_root

Subject: CN=desktop.example.com/unstructuredName=CA-router

PKI[9]: End sorted cert chain

PKI[13]: pki_ossl_get_store, pki_ossl_certstore.c:61

PKI[12]: pki_ossl_rebuild_ca_store, pki_ossl_certstore.c:194

PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:42

PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:42

PKI[14]: pki_ossl_get_cert_summary, pki_ossl.c:119

PKI[9]: Cert to verify

PKI[9]: -----Certificate-----:

Serial Number: 2 (0x2)

Issuer: O=cisco, OU=TAC, CN=calo_root

Subject: CN=desktop.example.com/unstructuredName=CA-router

PKI[12]: pki_verify_cb, pki_ossl_validate.c:358

PKI[8]: val status=1: cert subject: /O=cisco/OU=TAC/CN=calo_root. ctx->error: (0)ok, cert_idx: 1

PKI[12]: pki_verify_cb, pki_ossl_validate.c:358

PKI[8]: val status=1: cert subject: /CN=desktop.example.com/unstructuredName=CA-router. ctx->error: (0)

PKI[8]: pki_ossl_find_valid_chain took 167 microseconds

PKI[7]: session 0x06c8d45f, Validation with CRL checking completed, status 0

PKI[7]: session 0x06c8d45f, Revocation check complete, no revoked certs found

PKI[12]: pki_ossl_do_callback, pki_ossl_validate.c:164

PKI[13]: CERT_Close, vpn3k_cert_api.c:291

PKI[8]: Close session 0x06c8d45f asynchronously

PKI[13]: CERT_API_req_enqueue, vpn3k_cert_api.c:2913

PKI[9]: Async unlocked for session 0x06c8d45f

PKI[8]: No IOCB found for SOCKET_CLOSE message, handle 0x5dba666

PKI[12]: CERT_API_Q_Process, vpn3k_cert_api.c:2811

PKI[12]: CERT_API_process_req_msg, vpn3k_cert_api.c:2746

PKI[8]: process msg cmd=1, session=0x06c8d45f

PKI[9]: Async locked for session 0x06c8d45f

PKI[9]: Async unlocked for session 0x06c8d45f

PKI[13]: pki_ossl_free_valctx, pki_ossl_validate.c:251

PKI[13]: free_fsm_data, pki_ossl_revocation.c:225

PKI[13]: ocsf_free_fsmdata, pki_ossl_ocsp.c:1462

PKI[13]: free_fsm_data, pki_ossl_revocation.c:225

PKI[13]: ocsf_free_fsmdata, pki_ossl_ocsp.c:1462

PKI[9]: CERT_API thread sleeps!

PKI[13]: CERT_GetGroupFromSSLRule, vpn3k_cert_api.c:1672

Die nächste FTD-Erfassung zeigt die HTTP-Transaktion zwischen FTD und CDP (in diesem Fall CA-Server) an, um die Sperrliste abzurufen.

The screenshot shows a network capture in Wireshark. The packet list pane highlights packet 4, which is an HTTP GET request. The details pane for this packet is expanded, showing the following information:

- Request Method: GET
- Request URI: /cgi-bin/pkiclient.exe?operation=GetCRL
- Request URI Path: /cgi-bin/pkiclient.exe
- Request URI Query: operation=GetCRL
- Request Version: HTTP/1.0
- Host: 192.0.2.10\r\n
- [Full request URI: http://192.0.2.10/cgi-bin/pkiclient.exe?operation=GetCRL]
- [HTTP request 1/1]
- [Response in frame: 8]

The screenshot shows a network capture in Wireshark. The packet list pane highlights packet 8, which is a Certificate Revocation List (CRL) response. The details pane for this packet is expanded, showing the following information:

- signedCertificateList
 - signature (sha1WithRSAEncryption)
 - issuer: rdnSequence (0)
 - thisUpdate: utcTime (0)
 - nextUpdate: utcTime (0)
- algorithmIdentifier (sha1WithRSAEncryption)
 - Algorithm Id: 1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
 - Padding: 0
 - encrypted: 0a9b3a3e44674360c548fb7c6f058e7ba9687c99e16311dd2bfc8a31134e59b589cbe423...

Szenario 2. Das Zertifikat wird widerrufen, und die Authentifizierung schlägt fehl.

Ein Identitätszertifikat wird auf dem CA-Server widerrufen und in der CRL-Datenbankdatei registriert. Die aktualisierte Zertifikatsperrliste steht dem FTD jedoch erst nach Ablauf der

aktuellen Zertifikatsperrliste zur Verfügung (sie ist für zwei Stunden gültig).

<#root>

```
CA-router#show crypto pki server CAS crl
Certificate Revocation List:
Issuer: cn=calo_root,ou=TAC,o=cisco
This Update: 22:18:38 UTC Sep 24 2023
Next Update: 00:18:38 UTC Sep 25 2023

Number of CRL entries: 0
```

CRL size: 249 bytes

```
CA-router#show crypto pki server CAS certificates
Serial Issued date Expire date Subject Name
1 20:18:36 UTC Sep 24 2023 20:18:36 UTC Jun 20 2026 cn=calo_root ou=TAC o=cisco
2 20:19:33 UTC Sep 24 2023 20:19:33 UTC Jul 20 2024 hostname=CA-router cn=desktop.example.com

3 23:50:58 UTC Sep 24 2023 23:50:58 UTC Jul 20 2024 cn=test.cisco.com
```

CA-router#

```
crypto pki server CAS revoke 0x2
```

% Certificate 02 succesfully revoked.

```
CA-router#show crypto pki server CAS crl
Certificate Revocation List:
Issuer: cn=calo_root,ou=TAC,o=cisco
This Update: 23:59:32 UTC Sep 24 2023
Next Update: 01:59:32 UTC Sep 25 2023
Number of CRL entries: 1
CRL size: 272 bytes
```

Revoked Certificates:

Serial Number (hex): 02

Revocation Date: 23:59:32 UTC Sep 24 2023

Wenn Sie versuchen, eine neue Verbindung herzustellen, nachdem die Zertifikatsperrliste abgelaufen ist, ist die Zertifikatsprüfung größtenteils identisch mit dem vorherigen Szenario. Die neue Zertifikatsperrliste wird angefordert, nachdem die FTD bestätigt hat, dass sich keine Zertifikatsperrliste im Cache befindet. Nach Erhalt der neuen Zertifikatsperrliste prüft die FTD, ob die Seriennummer des Identitätsnachweises in der Liste enthalten ist. Die Seriennummer ist als gesperrt markiert, und die FTD verweigert dem Benutzer den Zugriff.

<#root>

CRYPTO_PKI: bitValue of KEY_USAGE = a0PKI[7]: CRYPTO_PKI:check_key_usage: Checking KU for case VPN peer
PKI[7]: CRYPTO_PKI:check_key_usage: KU bit digitalSignature is ON.
PKI[7]: ExtendedKeyUsage OID = serverAuth NOT acceptable for usage type SSL VPN Peer
PKI[7]: ExtendedKeyUsage OID = clientAuth acceptable for usage type: SSL VPN Peer
PKI[7]: check_key_usage:Extended Key/Key Usage check OK
PKI[12]: pki_ossl_revocation_check, pki_ossl_validate.c:931
PKI[7]: Starting revocation check for session 0x0dc288f9
PKI[12]: pki_init_revocation, pki_ossl_revocation.c:162
PKI[12]: pki_ossl_eval_revocation, pki_ossl_validate.c:699
PKI[7]: Evaluating session revocation status, 1 certs to check
PKI[8]: session 0x0dc288f9, cert 0 has rev_status 0, using methods 1/3/0 at index 0
PKI[12]: cert_revoc_exempt, pki_ossl_revocation.c:250
PKI[13]: get_tp_from_policy, pki_ossl_policy_transition.c:230
PKI[11]: polinfo->name: CRL-AC
PKI[11]: tp label: Trustpool
PKI[13]: label: CRL-AC
PKI[13]: pki_crl_cached, pki_ossl_crl_cache.c:1351
PKI[13]: get_tp_from_policy, pki_ossl_policy_transition.c:230
PKI[11]: polinfo->name: CRL-AC
PKI[11]: tp label: Trustpool
PKI[13]: label: CRL-AC
PKI[12]: pki_ossl_check_cache, pki_ossl_crl_cache.c:1269
PKI[7]: Starting OSSL CRL cache check.
PKI[12]: pki_ossl_crypto_build_crdp_list, pki_ossl_crl_cache.c:326
PKI[12]: pki_get_der_cdp_ext, crypto_pki.c:1528
PKI[14]: url_type_allowed, pki_ossl_crl_cache.c:153

PKI[9]: Attempting to find cached CRL for CDP http://192.0.2.10/cgi-bin/pkiclient.exe?operation=GetCRL

PKI[12]: pki_ossl_SelectCRLByIssuerTimeDER, pki_ossl_crl_cache.c:1219
PKI[14]: pki_ossl_get_name_string, pki_ossl.c:315
PKI[9]: Select DER crl(O=cisco, OU=TAC, CN=calo_root)
PKI[12]: pki_ossl_get_crl_internal, pki_ossl_crl_cache.c:506

PKI[7]: CRL not cached. Initiating CRL download for cert idx 0.

PKI[12]: do_get_crl, pki_ossl_revocation.c:85
PKI[9]: starting CRL FSM #0
PKI[11]: drive_fsm, pki_ossl_revocation.c:33
PKI[8]: [Sess: 0x0dc288f9, Cert: 0] FSM: In PKICRL_InitTransaction
PKI[12]: get_cdps, pki_crl_fsm_act.c:202
PKI[13]: get_tp_from_policy, pki_ossl_policy_transition.c:230
PKI[11]: polinfo->name: CRL-AC
PKI[11]: tp label: Trustpool
PKI[13]: label: CRL-AC
PKI[12]: pki_ossl_crypto_build_crdp_list, pki_ossl_crl_cache.c:326
PKI[12]: pki_get_der_cdp_ext, crypto_pki.c:1528
PKI[14]: url_type_allowed, pki_ossl_crl_cache.c:153

PKI[7]: cdp: (len=58, type=URI, prot=HTTP) http://192.0.2.10/cgi-bin/pkiclient.exe?operation=GetCRL

PKI[8]: [Sess: 0x0dc288f9, Cert: 0] FSM: PKICRL_InitTransaction, Return status: 0
PKI[8]: [Sess: 0x0dc288f9, Cert: 0] FSM: In PKICRL_NextCDP
PKI[12]: crldl_cdp_blacklisted, pki_ossl_crl.c:1374
PKI[12]: crl_find_pending_crl, pki_ossl_crl.c:1155
PKI[13]: get_pending_crl_list, pki_ossl_crl.c:1101
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:42
PKI[14]: cmp_cdp_info, pki_ossl_crl.c:1121
PKI[14]: cmp_cdp_info, pki_ossl_crl.c:1121
PKI[14]: cmp_cdp_info, pki_ossl_crl.c:1121
PKI[7]: CDP is not blacklisted

PKI[8]: [Sess: 0x0dc288f9, Cert: 0] FSM: PKICRL_NextCDP, Return status: 0
PKI[8]: [Sess: 0x0dc288f9, Cert: 0] FSM: In PKICRL_Request
PKI[13]: crldp_download_pending, pki_oss1_crl.c:1184
PKI[12]: crl_find_pending_crl, pki_oss1_crl.c:1155
PKI[13]: get_pending_crl_list, pki_oss1_crl.c:1101
PKI[13]: crypto_pki_get_oss1_env, pki_oss1.c:42
PKI[14]: cmp_cdp_info, pki_oss1_crl.c:1121
PKI[14]: cmp_cdp_info, pki_oss1_crl.c:1121
PKI[14]: cmp_cdp_info, pki_oss1_crl.c:1121
PKI[8]: session 0x0dc288f9 adding pending CRL entry for cert 0
PKI[12]: crldp_add_pending_download, pki_oss1_crl.c:1203
PKI[12]: crl_find_pending_crl, pki_oss1_crl.c:1155
PKI[13]: get_pending_crl_list, pki_oss1_crl.c:1101
PKI[13]: crypto_pki_get_oss1_env, pki_oss1.c:42
PKI[14]: cmp_cdp_info, pki_oss1_crl.c:1121
PKI[14]: cmp_cdp_info, pki_oss1_crl.c:1121
PKI[14]: cmp_cdp_info, pki_oss1_crl.c:1121
PKI[13]: get_pending_crl_list, pki_oss1_crl.c:1101
PKI[13]: crypto_pki_get_oss1_env, pki_oss1.c:42
PKI[12]: retrieve_crl, pki_crl_fsm_act.c:233
PKI[13]: get_tp_from_policy, pki_oss1_policy_transition.c:230
PKI[11]: polinfo->name: CRL-AC
PKI[11]: tp label: Trustpool
PKI[13]: label: CRL-AC

PKI[7]: CDP type HTTP

PKI[7]: getting http://192.0.2.10/cgi-bin/pkiclient.exe?operation=GetCRL

PKI[12]: pki_oss1_crl_build_http_io, pki_oss1_crl.c:1017
PKI[13]: pki_parse_uri, pki_oss1_uri.c:75
PKI[14]: pki_uri_map_protocol, pki_oss1_uri.c:17
PKI[14]: pki_uri_get_port, pki_oss1_uri.c:34
PKI[13]: pki_free_uri, pki_oss1_uri.c:57
PKI[11]: pki_crl_request_send_async, pki_oss1_crl.c:627

PKI[8]: [16] IOCB allocated

PKI[7]: PKI CRL I/O request queue result: IO_STATUS_QUEUEED

PKI[8]: [Sess: 0x0dc288f9, Cert: 0] FSM: PKICRL_Request, Return status: 0

PKI[7]: Chain revocation status: good: 0, exempt: 0, cached: 0, revoked: 0, error: 0, pending: 1, fail-

PKI[9]: Async unlocked for session 0x0dc288f9

PKI[8]: [16] Received IO request msg

PKI[8]: [16] DNS resolve issued for 192.0.2.10

PKI[9]: CERT API thread sleeps!

PKI[7]: [16] DNS resolve 192.0.2.10 (192.0.2.10)

PKI[8]: [16] Socket open success

PKI[8]: [16] IPv4 Route lookup to 192.0.2.10 use interface outside

PKI[8]: [16] Connect sent to 192.0.2.10 from 192.0.2.1

PKI[12]: pki_io_cbfunc_log_revocation_check, pki_oss1_revocation.c:421

PKI[7]: 6717056: Attempting CRL revocation check from outside:192.0.2.1/27791 to 192.0.2.10/80 using HT

PKI[8]: [16] Received Socket transmit ready msg

----- Begin Data Type:HTTP Request [16]

Length: 76 -----

47 45 54 20 2f 63 67 69 2d 62 69 6e 2f 70 6b 69 | GET /cgi-bin/pki
63 6c 69 65 6e 74 2e 65 78 65 3f 6f 70 65 72 61 | client.exe?opera
74 69 6f 6e 3d 47 65 74 43 52 4c 20 48 54 54 50 | tion=GetCRL HTTP
2f 31 2e 30 0d 0a 48 6f 73 74 3a 20 31 39 32 2e | /1.0..Host: 192.
31 38 31 2e 33 2e 31 30 0d 0a 0d 0a | 0.2.10....

----- End Data Type:HTTP Request [16]

Length: 76 -----

PKI[8]: [16] Sent 76 bytes

PKI[8]: [16] Received Socket read ready msg

PKI[8]: [16] read 685 bytes

PKI[8]: [16] Read EOF

PKI[12]: pki_io_cbfunc, pki_crl_fsm_act.c:59

PKI[7]: Callback received for vcid: 0, sess_id: 0x0dc288f9, cert_idx: 0, status: IO_STATUS_OK(1), data1

PKI[13]: get_fsm_data, pki_ossl_revocation.c:446

PKI[7]: [16] IOCB freed

PKI[13]: CERT_API_QueueFSMEvent, vpn3k_cert_api.c:137

PKI[13]: CERT_API_req_enqueue, vpn3k_cert_api.c:2913

PKI[9]: CERT API thread wakes up!

PKI[12]: CERT_API_Q_Process, vpn3k_cert_api.c:2811

PKI[12]: CERT_API_process_req_msg, vpn3k_cert_api.c:2746

PKI[8]: process msg cmd=2, session=0x0dc288f9

PKI[9]: Async locked for session 0x0dc288f9

PKI[11]: pki_notify_fsm_evt, pki_ossl_revocation.c:56

PKI[11]: drive_fsm, pki_ossl_revocation.c:33

PKI[8]: [Sess: 0x0dc288f9, Cert: 0] FSM: In PKICRL_ProcessResp

PKI[13]: pki_ossl_util_find_http_payload, pki_ossl_utils.c:36

PKI[8]: Received CRL of length 272 for session 0x0dc288f9, cert idx 0

PKI[13]: get_tp_from_policy, pki_ossl_policy_transition.c:230

PKI[11]: polinfo->name: CRL-AC

PKI[11]: tp label: Trustpool

PKI[13]: label: CRL-AC

PKI[12]: pki_ossl_crl_add_to_cache, pki_ossl_crl_cache.c:1177

PKI[12]: pki_ossl_crypto_verify_and_insert_crl, pki_ossl_crl_cache.c:1126

PKI[12]: pki_ossl_insert_der_crl_int, pki_ossl_crl_cache.c:1017

PKI[8]: Inserting CRL

PKI[14]: pki_ossl_get_crl_summary, pki_ossl.c:151

PKI[8]: -----CRL-----:

Certificate Revocation List (CRL):

Version 1 (0x0)

Signature Algorithm: sha1WithRSAEncryption

Issuer: /O=cisco/OU=TAC/CN=calo_root

Last Update: Sep 25 00:18:09 2023 GMT

Next Update: Sep 25 02:18:09 2023 GMT

Number of Revoked Certificates: 1

PKI[12]: asn1_to_unix_time, crypto_pki.c:1735

PKI[12]: asn1_to_unix_time, crypto_pki.c:1735

PKI[12]: pki_ossl_crypto_certc_insert_CRL, pki_ossl_crl_cache.c:735

PKI[7]: CRL: current time is 1695601164

PKI[7]: CRL: nextupdate time is 1695608289

PKI[7]: CRL: lastupdate time is 1695601089

PKI[7]: set CRL update timer with delay: 7125

PKI[7]: ExtendedKeyUsage OID = clientAuth acceptable for usage type: SSL VPN Peer
PKI[7]: check_key_usage:Extended Key/Key Usage check OK
PKI[12]: pki_ossl_revocation_check, pki_ossl_validate.c:931
PKI[7]: Starting revocation check for session 0x1acca1bd
PKI[12]: pki_init_revocation, pki_ossl_revocation.c:162
PKI[12]: pki_ossl_eval_revocation, pki_ossl_validate.c:699
PKI[7]: Evaluating session revocation status, 1 certs to check
PKI[8]: session 0x1acca1bd, cert 0 has rev_status 0, using methods 1/3/0 at index 0
PKI[12]: cert_revoc_exempt, pki_ossl_revocation.c:250
PKI[13]: get_tp_from_policy, pki_ossl_policy_transition.c:230
PKI[11]: polinfo->name: CRL-AC
PKI[11]: tp label: Trustpool
PKI[13]: label: CRL-AC
PKI[13]: pki_crl_cached, pki_ossl_crl_cache.c:1351
PKI[13]: get_tp_from_policy, pki_ossl_policy_transition.c:230
PKI[11]: polinfo->name: CRL-AC
PKI[11]: tp label: Trustpool
PKI[13]: label: CRL-AC
PKI[12]: pki_ossl_check_cache, pki_ossl_crl_cache.c:1269
PKI[7]: Starting OSSL CRL cache check.
PKI[12]: pki_ossl_crypto_build_crl_dp_list, pki_ossl_crl_cache.c:326
PKI[12]: pki_get_der_cdp_ext, crypto_pki.c:1528
PKI[14]: url_type_allowed, pki_ossl_crl_cache.c:153

PKI[9]: Attempting to find cached CRL for CDP http://192.0.2.10/cgi-bin/pkiclient.exe?operation=GetCRL

PKI[12]: pki_ossl_SelectCRLByIssuerTimeDER, pki_ossl_crl_cache.c:1219
PKI[14]: pki_ossl_get_name_string, pki_ossl.c:315
PKI[9]: Select DER crl(O=cisco, OU=TAC, CN=calo_root)
PKI[12]: pki_ossl_get_crl_internal, pki_ossl_crl_cache.c:506
PKI[13]: is_crl_dst, pki_ossl_crl_cache.c:479
PKI[7]: CRL for cert idx 0 found in cache
PKI[7]: Chain revocation status: good: 0, exempt: 0, cached: 1, revoked: 0, error: 0, pending: 0, fail-
PKI[7]: session: 0x1acca1bd, all revocation processing complete
PKI[5]: session: 0x1acca1bd, CRL for certificate 0 has been cached
PKI[12]: pki_ossl_rebuild_ca_store, pki_ossl_certstore.c:194
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:42

PKI[7]: session 0x1acca1bd, Starting chain validation with cached CRL checking

PKI[12]: pki_ossl_find_valid_chain, pki_ossl_validate.c:472
PKI[9]: Begin sorted cert chain
PKI[14]: pki_ossl_get_cert_summary, pki_ossl.c:119
PKI[9]: -----Certificate-----:
Serial Number: 1 (0x1)
Issuer: O=cisco, OU=TAC, CN=calo_root
Subject: O=cisco, OU=TAC, CN=calo_root

PKI[14]: pki_ossl_get_cert_summary, pki_ossl.c:119
PKI[9]: -----Certificate-----:
Serial Number: 2 (0x2)
Issuer: O=cisco, OU=TAC, CN=calo_root
Subject: CN=desktop.example.com/unstructuredName=CA-router

PKI[9]: End sorted cert chain
PKI[13]: pki_ossl_get_store, pki_ossl_certstore.c:61
PKI[12]: pki_ossl_rebuild_ca_store, pki_ossl_certstore.c:194
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:42
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:42
PKI[14]: pki_ossl_get_cert_summary, pki_ossl.c:119
PKI[9]: Cert to verify

```
PKI[9]: -----Certificate-----:
Serial Number: 2 (0x2)
Issuer: O=cisco, OU=TAC, CN=ca1o_root
Subject: CN=desktop.example.com/unstructuredName=CA-router

PKI[12]: pki_verify_cb, pki_oss1_validate.c:358

PKI[6]: val status=0: cert subject: /CN=desktop.example.com/unstructuredName=CA-router. ctx->error: (23)

PKI[14]: is_crl_error, pki_oss1_validate.c:278
PKI[14]: is_crl_error, pki_oss1_validate.c:278

PKI[4]: Certificate verification error: certificate revoked

PKI[14]: map_oss1_error, pki_oss1_validate.c:62
PKI[7]: session 0x1acca1bd, Validation with CRL checking completed, status 15
PKI[5]: session 0x1acca1bd, Error in revocation check or revoked certs found
PKI[12]: pki_oss1_do_callback, pki_oss1_validate.c:164
PKI[13]: CERT_Close, vpn3k_cert_api.c:291
PKI[8]: Close session 0x1acca1bd asynchronously
PKI[13]: CERT_API_req_enqueue, vpn3k_cert_api.c:2913
PKI[9]: Async unlocked for session 0x1acca1bd
PKI[12]: CERT_API_Q_Process, vpn3k_cert_api.c:2811
PKI[12]: CERT_API_process_req_msg, vpn3k_cert_api.c:2746
PKI[8]: process msg cmd=1, session=0x1acca1bd
PKI[9]: Async locked for session 0x1acca1bd
PKI[9]: Async unlocked for session 0x1acca1bd
PKI[13]: pki_oss1_free_valctx, pki_oss1_validate.c:251
PKI[13]: free_fsm_data, pki_oss1_revocation.c:225
PKI[13]: oosp_free_fsmdata, pki_oss1_oosp.c:1462
PKI[13]: free_fsm_data, pki_oss1_revocation.c:225
PKI[13]: oosp_free_fsmdata, pki_oss1_oosp.c:1462
PKI[9]: CERT API thread sleeps!
```

Die nächste FTD-Erfassung zeigt die HTTP-Transaktion zwischen FTD und CDP an, um die Sperrliste abzurufen, nachdem ein gesperrtes Zertifikat in der Liste gespeichert ist.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
4	0.000152	192.0.2.1	192.0.2.10	HTTP	140	GET /cgi-bin/pkiclient.exe?operation
5	0.000733	192.0.2.10	192.0.2.1	TCP	66	80 → 57791 [ACK] Seq=1 Ack=75 Win=2
6	0.004821	192.0.2.10	192.0.2.1	TCP	751	80 → 57791 [PSH, ACK] Seq=1 Ack=75
7	0.000107	192.0.2.1	192.0.2.10	TCP	66	57791 → 80 [ACK] Seq=75 Ack=686 Win
8	0.000015	192.0.2.10	192.0.2.1	PKIX-CRL	66	Certificate Revocation List
9	0.000092	192.0.2.1	192.0.2.10	TCP	66	57791 → 80 [ACK] Seq=75 Ack=687 Win
10	0.000046	192.0.2.1	192.0.2.10	TCP	66	57791 → 80 [FIN, PSH, ACK] Seq=75 A
11	0.000625	192.0.2.10	192.0.2.1	TCP	66	80 → 57791 [ACK] Seq=687 Ack=76 Win

```

X-XSS-Protection: 1; mode=block\r\n
X-Content-Type-Options: nosniff\r\n
X-Frame-Options: SAMEORIGIN\r\n
\r\n
[HTTP response 1/1]
[Time since request: 0.005676000 seconds]
[Request in frame: 4]
[Request URI: http://192.0.2.10/cgi-bin/pkiclient.exe?operation=GetCRL]
File Data: 272 bytes
Certificate Revocation List
  signedCertificateList
    > signature (sha1WithRSAEncryption)
    > issuer: rdnSequence (0)
    > thisUpdate: utcTime (0)
    > nextUpdate: utcTime (0)
    > revokedCertificates: 1 item
      > revokedCertificates item
        userCertificate: 0x02
        > revocationDate: utcTime (0)
    > algorithmIdentifier (sha1WithRSAEncryption)
    Padding: 0
    encrypted: 7b049a1dc049f4b08c16eb35c5de48f01324a42763bf4ea72404d3c43a0cf72a20dc2fff...

```

Fehlerbehebung

Diese Befehle können verwendet werden, um weitere Probleme im Zusammenhang mit Zertifikaten zu identifizieren:

- Zur FTD:

```
debug crypto ca 14
```

- Auf dem CA-Router:

```

debug crypto pki API
debug crypto pki callbacks
debug crypto pki messages
debug crypto pki validation
debug crypto pki error
debug crypto pki server

```

debug crypto pki transactions

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.