Troubleshoot CRL for AnyConnect Certificate Based Authentication

Contents

Introduction

This document describes how to troubleshoot the Certificate Revocation List (CRL) configured for AnyConnect certificate-based authentication.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Certificate Authority (CA)
- Public Key Infrastructure (PKI)
- RA VPN on FTD
- Windows 10 with AnyConnect Client

Components Used

The information in this document is based on these software versions:

- CSR1000V - Cisco IOS® XE, Version 16.12.03 - as Cisco IOS XE CA Server
- NGFWv - Version 7.1.0 - as VPN gateway
- AnyConnect Secure Mobility Client version 4.10.07073- as the VPN client
- Windows 10 as a local computer

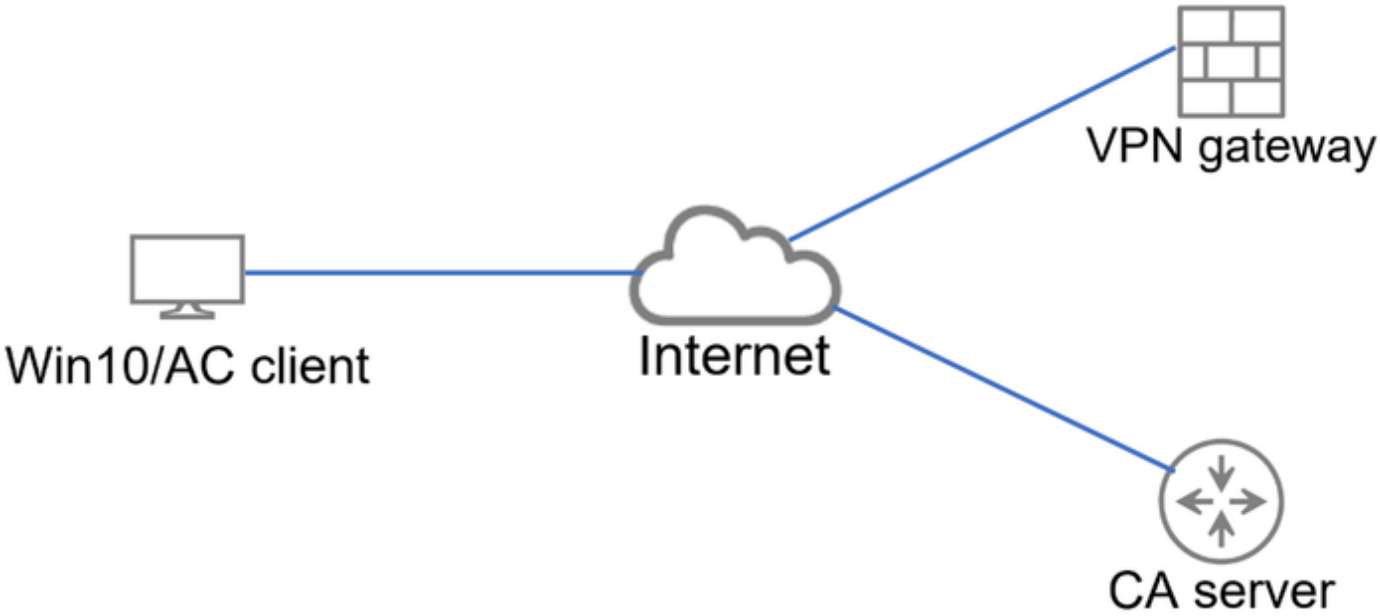
The information in this document was created from the devices in a specific lab environment. All of the

devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

CRL enables devices to determine if a certificate has been revoked before the lifetime of the certificate expires. A CRL contains the serial number and the revocation date of the certificate. A secure gateway such as Firepower Thread Defense (FTD) systems or other end devices uses this feature in order to strengthen the certificate authentication by validating the certificate status.

Topology



Basic topology that provides connectivity to the VPN gateway and CA server.

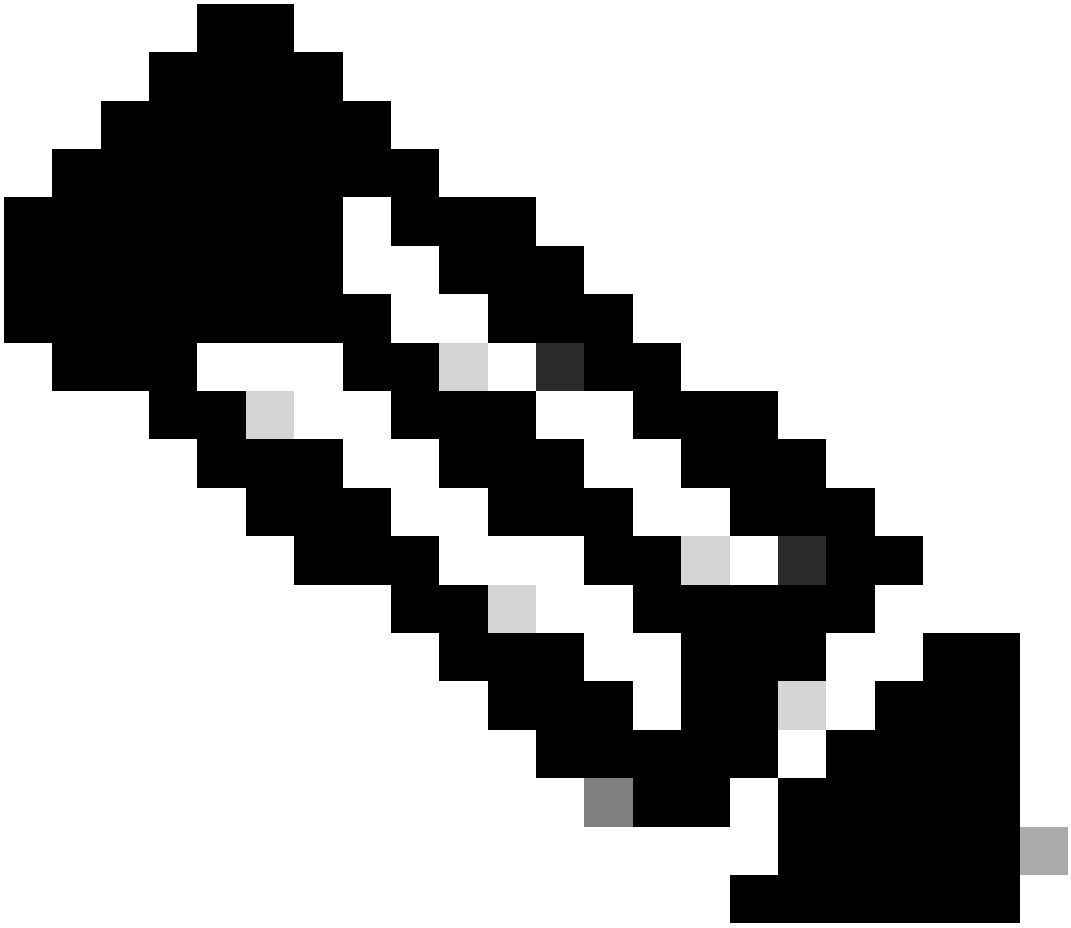
Important Configuration

In order to accomplish certificate-based Authentication with CRL, the presented configuration was used in each of the devices involved.

CA Router

The Server Certificate Authority is responsible for issuing identity certificates to the users in order to provide authentication against the VPN gateway. Additionally, the router stores the CRL database file and acts as the CRL distribution Point (CDP).

A CDP is where the VPN gateway and other end-users retrieve the CRL information. This information is cached locally and is valid only for a specific period of time; when this time expires, a new CRL is downloaded.



Note: The CRL database and the location where the devices have access to the CRL can be on the same device. However, it is recommended for security reasons that the CRL the end-devices access to is stored in a different device than the CRL database. In this example, the CA router stores the CRL database and acts as CDP for the 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
```

VPN Gateway Configuration

The FTD is configured in order to provide a Remote Access VPN to the end-users using certificates as the authentication method (certificate only). Upon receiving the identity certificate from the user, the FTD verifies if the certificate was issued by a known Certificate Authority (CA) and confirms its validity by getting the CRL from the CDP defined in the certificate.

<#root>

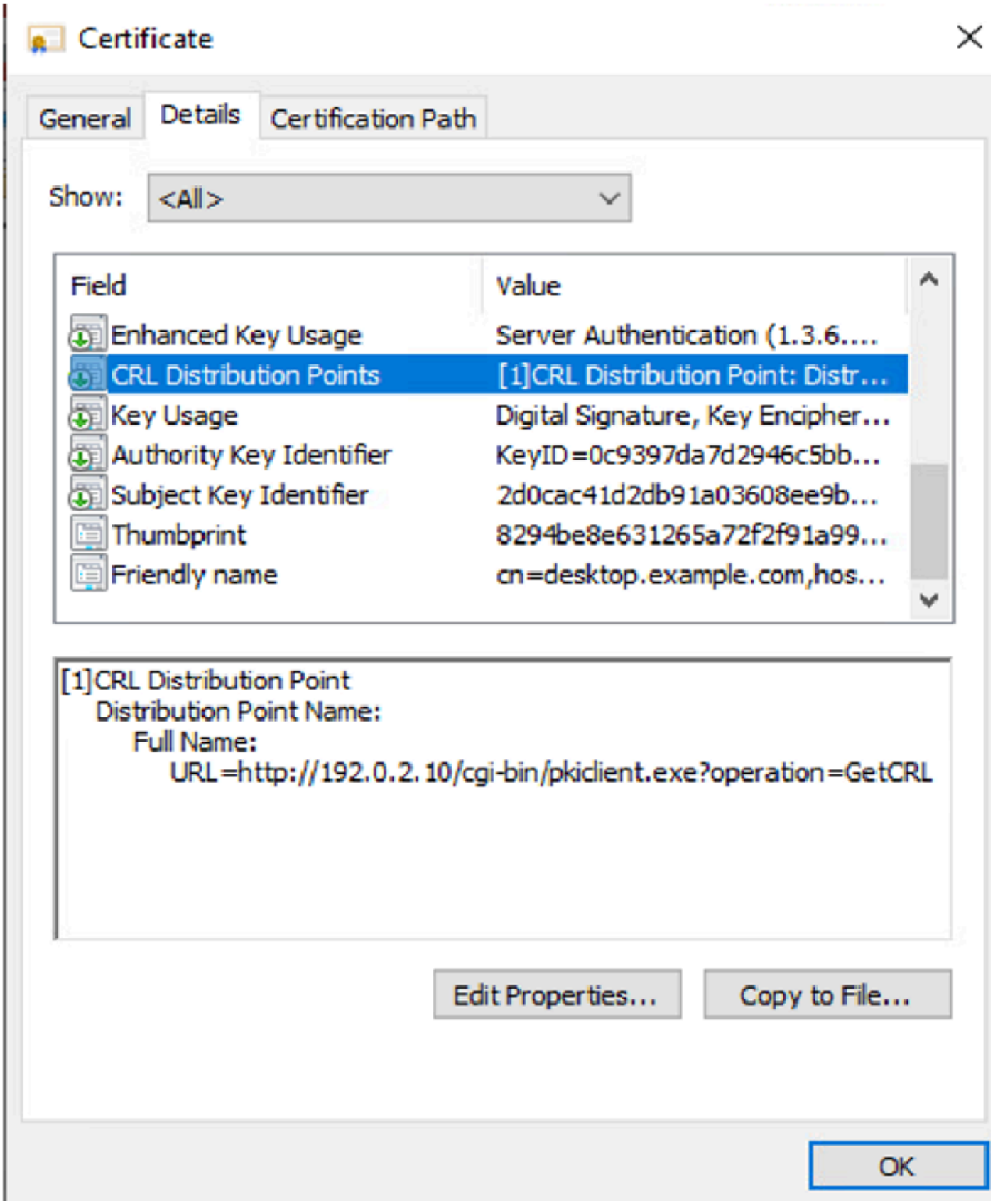
```
tunnel-group local type remote-access
tunnel-group local general-attributes
address-pool AC_pool
default-group-policy local_gp
username-from-certificate use-entire-name
tunnel-group local_test webvpn-attributes
```

authentication certificate

```
group-alias test enable
```

Windows Device

An identity certificate was issued by the CA server and installed into the Windows device.



Validation

The next debugs and captures display the difference between a user using a valid certificate (working scenario) and a user using a certificate that has been revoked (non-working scenario).

Scenario 1. The Certificate Is Valid for Authentication

When the user starts the connection attempt, it provides to the FTD its identity certificate, the VPN gateway verifies the issuer is a known authority and starts requesting the CRL from the CDP defined in the identity certificate via HTTP/GET request. The CA server replies with the CRL and the FTD checks if the Serial Number of the certificate is listed. Since the CRL is empty (no revoked certificates) the FTD accepts the certificate as valid and allows the user to authenticate.

<#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_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 217 microsecs
PKI[6]: Verified chain:
PKI[14]: pki_ossl_get_cert_summary, pki_ossl.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_ossl_get_cert_summary, pki_ossl.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_ossl_revocation_check, pki_ossl_validate.c:931
PKI[7]: Starting revocation check for session 0x06c8d45f
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 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_crldp_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_crldp_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]: 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: 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_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[13]: get_pending_crl_list, pki_ossl_crl.c:1101
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:42
PKI[12]: retrieve_crl, pki_crl_fsm_act.c:233
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[7]: CDP type HTTP

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

```
PKI[12]: pki_ossl_crl_build_http_io, pki_ossl_crl.c:1017
PKI[13]: pki_parse_uri, pki_ossl_uri.c:75
PKI[14]: pki_uri_map_protocol, pki_ossl_uri.c:17
PKI[14]: pki_uri_get_port, pki_ossl_uri.c:34
PKI[13]: pki_free_uri, pki_ossl_uri.c:57
PKI[11]: pki_crl_request_send_async, pki_ossl_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_ossl_revocation.c:421
```

PKI[7]: 6717056: Attempting CRL revocation check from outside:192.0.2.1/62075 to 192.0.2.10/80 using HTT

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), datal
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

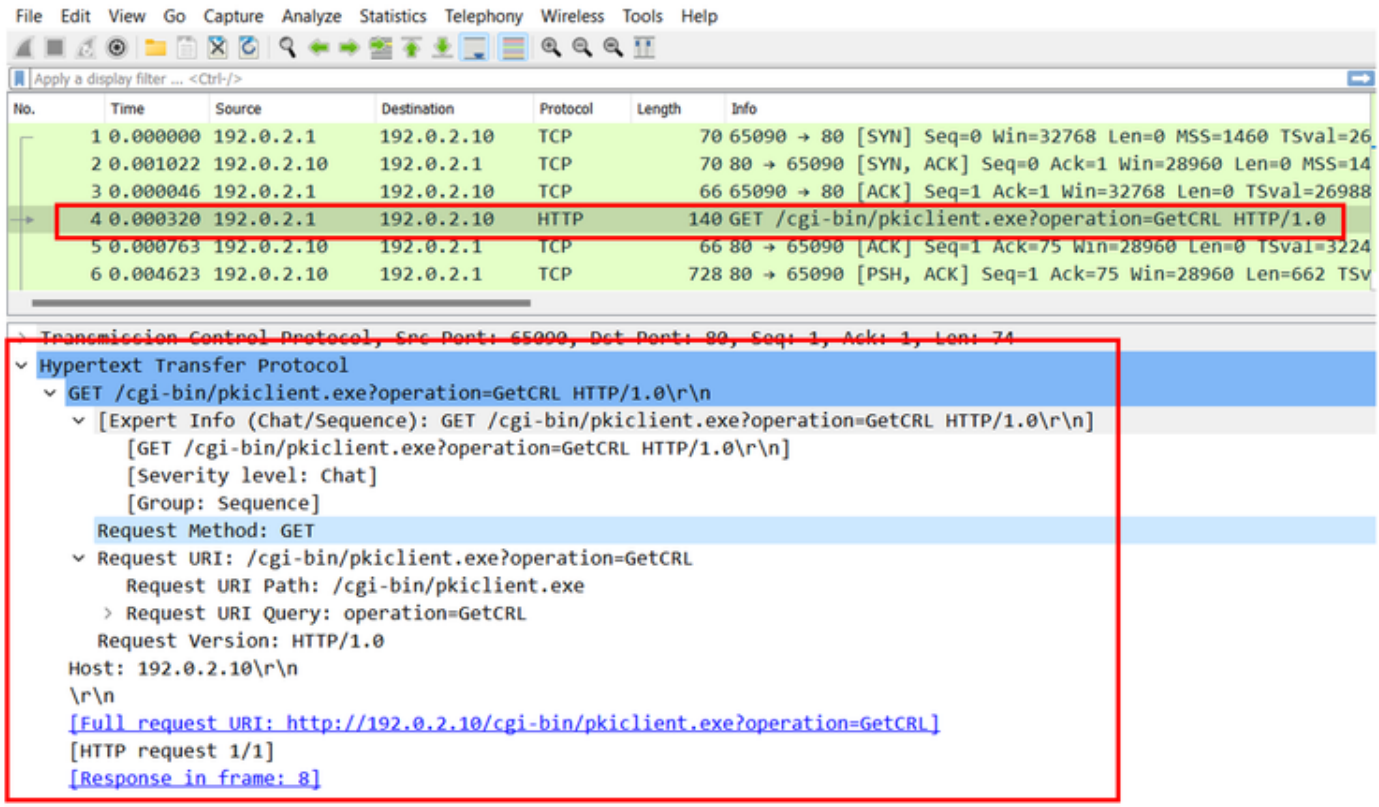
```
Subject: CN=desktop.example.com/unstructuredName=CA-router

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 microsecs
```

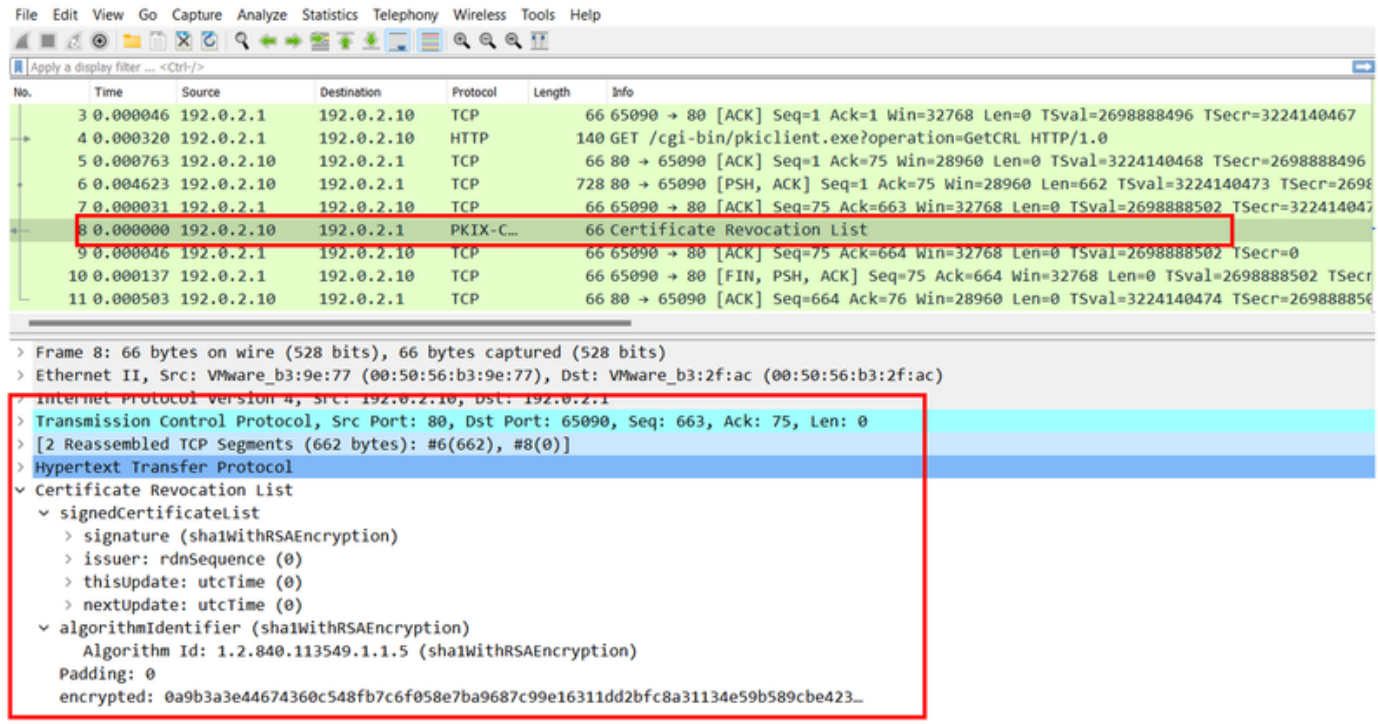
PKI[7]: session 0x06c8d45f, Validation with CRL checking completed, status 0

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]: ocsp_free_fsmdata, pki_ossl_ocsp.c:1462
PKI[13]: free_fsm_data, pki_ossl_revocation.c:225
PKI[13]: ocsp_free_fsmdata, pki_ossl_ocsp.c:1462
PKI[9]: CERT API thread sleeps!
PKI[13]: CERT_GetGroupFromSSLRule, vpn3k_cert_api.c:1672
```

The next FTD capture displays the HTTP transaction between the FTD and CDP (CA server in this case) in order to retrieve the CRL.





Scenario 2. The Certificate Is Revoked and Authentication Fails

An identity certificate is revoked in the CA server and registered in the CRL database file. However, the updated CRL is not available to the FTD until the current CRL expires (configured to be valid for two hours).

```
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
```

When attempting a new connection after confirming the CRL expired, the certificate inspection is mostly identical to the previous scenario. The new CRL is requested after the FTD confirms there is no CRL in the cache. Upon receiving the new CRL the FTD checks whether the Serial Number of the identity certificate is part of the list. The Serial Number is marked as revoked and the FTD proceeds to deny access to the user.

<#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_crldp_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_crldp_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_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 0x0dc288f9 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_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[13]: get_pending_crl_list, pki_ossl_crl.c:1101
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:42
PKI[12]: retrieve_crl, pki_crl_fsm_act.c:233
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[7]: CDP type HTTP

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

```
PKI[12]: pki_ossl_crl_build_http_io, pki_ossl_crl.c:1017
PKI[13]: pki_parse_uri, pki_ossl_uri.c:75
PKI[14]: pki_uri_map_protocol, pki_ossl_uri.c:17
PKI[14]: pki_uri_get_port, pki_ossl_uri.c:34
PKI[13]: pki_free_uri, pki_ossl_uri.c:57
PKI[11]: pki_crl_request_send_async, pki_ossl_crl.c:627
PKI[8]: [16] IOCB allocated
PKI[7]: PKI CRL I/O request queue result: IO_STATUS_QUEUED
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_ossl_revocation.c:421
```

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

```
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), datal
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[12]: pki_ossl_get_crl_internal, pki_ossl_crl_cache.c:506
PKI[7]: the current device time: 00:19:24 UTC Sep 25 2023
PKI[7]: the last CRL update time: 00:18:09 UTC Sep 25 2023
PKI[7]: the next CRL update time: 02:18:09 UTC Sep 25 2023
PKI[7]: CRL cache delay being set to: 3600000
PKI[14]: pki_ossl_set_crl_store_dirty, pki_ossl_crl_cache.c:1441
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:42
PKI[12]: crldl_notify_result, pki_ossl_crl.c:1304
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[14]: cmp_cdp_info, pki_ossl_crl.c:1121
PKI[13]: get_pending_crl_list, pki_ossl_crl.c:1101
PKI[13]: crypto_pki_get_ossl_env, pki_ossl.c:42
PKI[8]: [Sess: 0x0dc288f9, Cert: 0] FSM: PKICRL_ProcessResp, Return status: 0
PKI[8]: [Sess: 0x0dc288f9, Cert: 0] FSM: In PKICRL_Callback
PKI[12]: rev_cb, pki_ossl_validate.c:902
PKI[7]: revocation status queued for session 0x0dc288f9 and cert_idx 0, rev_status 3
PKI[13]: CERT_API_QueueFSMResp, vpn3k_cert_api.c:158
PKI[13]: CERT_API_req_enqueue, vpn3k_cert_api.c:2913
PKI[8]: [Sess: 0x0dc288f9, Cert: 0] FSM: PKICRL_Callback, Return status: 0
PKI[9]: Async unlocked for session 0x0dc288f9
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=3, session=0x0dc288f9
PKI[9]: Async locked for session 0x0dc288f9
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 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: 0x0dc288f9, all revocation processing complete
PKI[5]: session: 0x0dc288f9, 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 0x0dc288f9, 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[6]: val status=0: cert subject: /CN=desktop.example.com/unstructuredName=CA-router. ctx->error: (23
PKI[14]: is_crl_error, pki_ossl_validate.c:278
PKI[14]: is_crl_error, pki_ossl_validate.c:278
PKI[4]: Certificate verification error: certificate revoked<<<<<<<<<<<<<<<<<<
PKI[14]: map_ossl_error, pki_ossl_validate.c:62
```

```
PKI[7]: session 0x0dc288f9, Validation with CRL checking completed, status 15
PKI[5]: session 0x0dc288f9, Error in revocation check or 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 0x0dc288f9 asynchronously
PKI[13]: CERT_API_req_enqueue, vpn3k_cert_api.c:2913
PKI[9]: Async unlocked for session 0x0dc288f9
PKI[8]: No IOCB found for SOCKET CLOSE message, handle 0x1a6b367e
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=0x0dc288f9
PKI[9]: Async locked for session 0x0dc288f9
PKI[9]: Async unlocked for session 0x0dc288f9
PKI[13]: pki_ossl_free_valctx, pki_ossl_validate.c:251
PKI[13]: free_fsm_data, pki_ossl_revocation.c:225
PKI[13]: ocsp_free_fsmdata, pki_ossl_ocsp.c:1462
PKI[13]: free_fsm_data, pki_ossl_revocation.c:225
PKI[13]: ocsp_free_fsmdata, pki_ossl_ocsp.c:1462
PKI[9]: CERT API thread sleeps!


[..output ommitted]

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_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 233 microsecs
PKI[6]: Verified chain:
PKI[14]: pki_ossl_get_cert_summary, pki_ossl.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_ossl_get_cert_summary, pki_ossl.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

[..ooutput 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_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_crldp_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=calo_root
Subject: CN=desktop.example.com/unstructuredName=CA-router

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

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

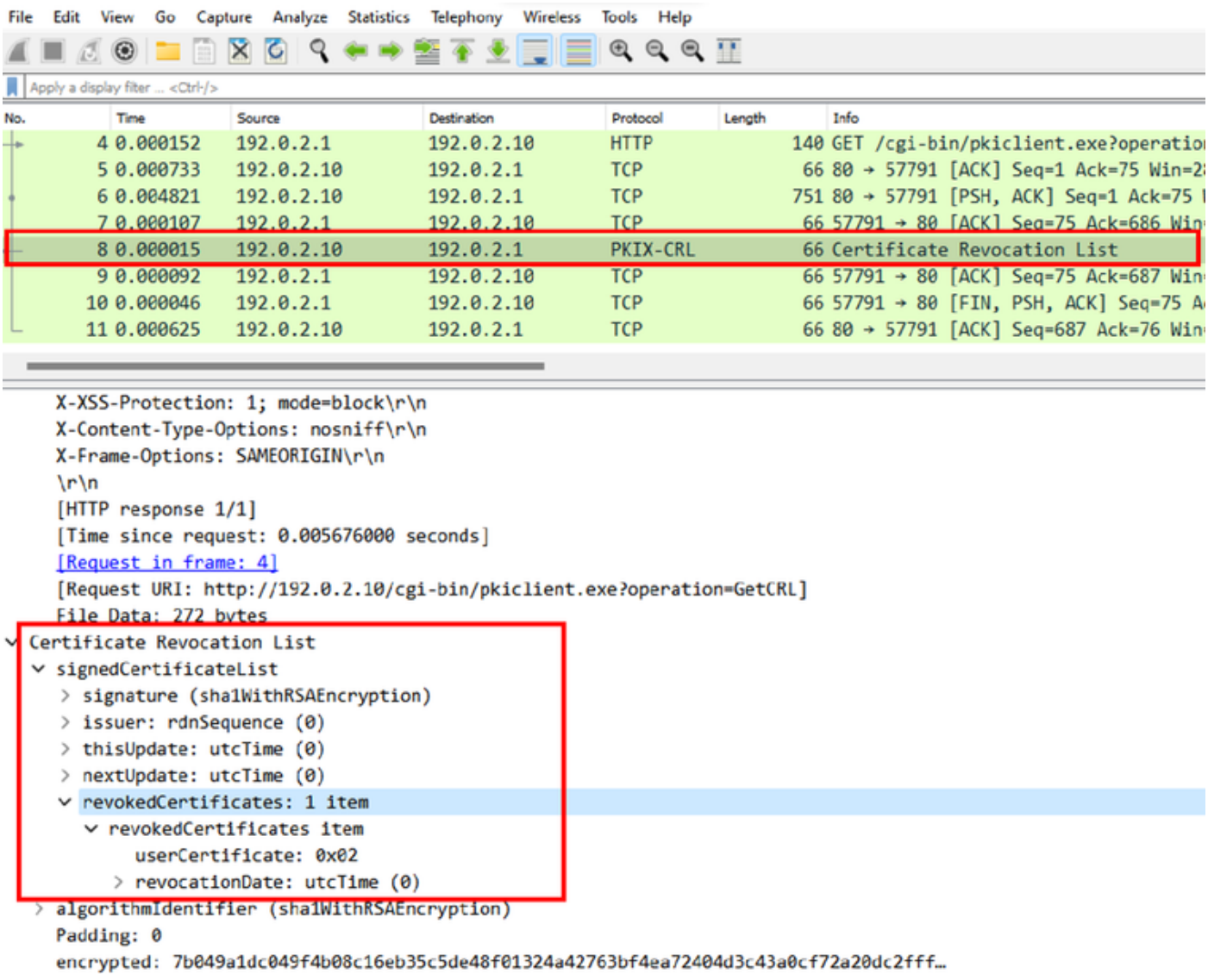
```
PKI[14]: is_crl_error, pki_ossl_validate.c:278
```

```
PKI[14]: is_crl_error, pki_ossl_validate.c:278
```

PKI[4]: Certificate verification error: certificate revoked

```
PKI[14]: map_ossl_error, pki_ossl_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_ossl_do_callback, pki_ossl_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_ossl_free_valctx, pki_ossl_validate.c:251
PKI[13]: free_fsm_data, pki_ossl_revocation.c:225
PKI[13]: ocsp_free_fsmdata, pki_ossl_ocsp.c:1462
PKI[13]: free_fsm_data, pki_ossl_revocation.c:225
PKI[13]: ocsp_free_fsmdata, pki_ossl_ocsp.c:1462
PKI[9]: CERT API thread sleeps!
```

The next FTD capture displays the HTTP transaction between the FTD and CDP in order to retrieve the CRL now that there is a revoked certificate stored in the list.



Troubleshoot

These commands can be used in order to identify further problems related to certificates:

- On the FTD:

```
debug crypto ca 14
```

- On the 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
```