Resolve IOS XE Certificate Validation Failures Due to CDP URL Mismatch with Multiple CRL Download URL

Contents

Issue

After additional CRL download URL locations are added to a Dynamic Multipoint VPN (DMVPN) hub device, some spoke tunnels fail to establish due to IKE negotiation failure and the hub logged this error:

```
%PKI-3-CERTIFICATE_INVALID: Certificate chain validation has failed
```

Although certificate chain validation succeeds and CRLs are successfully downloaded, revocation checking intermittently fail with:

```
No CRL found with matching CDP
revocation status = 2
```

This issue occurs when the DMVPN hub router uses multiple Certificate Revocation List (CRL) download URL locations pointing to the same CRL file. The CRL download locations include both IP-based and FQDN-based URLs, while the certificate issued to the spoke routers only has the FQDN-based URL in its CRL Distribution Point (CDP).

Environment

- Cisco devices running IOS® XE software configured for IPsec using certificate-based IKE authentication.
- Multiple CRL download locations with both IP-based and FQDN-based URLs hosting the same CRL files.
- Certificate issued to the peer devices only has the one URL in its CDP.

- IPsec tunnel configuration using certificate based authentication while enforcing Certificate Revocation check.

Resolution

The resolution involves standardizing on a single canonical CDP URL across the PKI environment to ensure exact URL matching during CRL validation.

Recommended Implementation Steps

1. Remove IP-based CRL Download URLs from Hub Configuration, if such IP-based CRL URLs are not Part of the Certificate CDP

```
no crypto pki crl download url http://x.x.x.x/prod/Example%20Company%20Issuing%20CA1.crl
no crypto pki crl download url http://x.x.x.x/prod/Example%20Company%20Issuing%20CA2.crl
```

2. Configure only FQDN-based CRL Download URLs that Match the CDP in the Spoke Certificates

```
crypto pki crl download url http://crl.examplecompnay.com/prod/Example%20Company%20Issuing%20CA1.crl
crypto pki crl download url http://crl.examplecompany.com/prod/Example%20Company%20Issuing%20CA2.crl
```

3. Update Issuing CA Templates to Use Consistent CDP URLs

Ensure the issuing CA templates stamp only the FQDN-based CDP URL into newly issued certificates.

4. Re-enroll Hub and Spoke Certificates (If Changing to New CDP URL)

If implementing a new CDP URL, change the issuing CA to publish the new CDP URL and re-enroll both hub and spoke certificates to carry the new URL.

Redundancy Implementation

For CRL provider redundancy, for example, to have the same CRL published at different URL locations to protect against failures on the hosting devices, implement backend redundancy behind a single FQDN using:

- DNS failover
- Load balancer
- Redundant CRL infrastructure

Do not use multiple CDPs with different hostnames/IPs as IOS XE treats these as different CDPs even if they reference the same CRL file.

Verification

After implementing the changes, verify CRL caching and tunnel establishment:

```
show crypto pki crl
```

Confirm that IKEv2 session establishes successfully:

```
show crypto session details
```

Cause

The issue is caused by IOS XE exact CDP URL matching behavior during CRL validation. When validating a peer certificate with revocation-check crl enabled, IOS XE performs an exact string match between the CDP URL embedded in the certificate being validated and the CDP URL associated with the CRL stored in the hub's parsed CRL cache.

This failure sequence occurs:

1. Hub successfully downloads CRL using IP-based CDP URL and caches it internally under that URL.
2. Spoke certificates reference the FQDN-based URL in its CDP.
3. During revocation validation, IOS XE searches for a cached CRL matching the FQDN URL.
4. No exact match is found because IOS XE treats IP-based and FQDN-based URLs as different CDPs.
5. Router returns "No CRL found with matching CDP" with revocation status = 2.
6. Certificate validation fails with %PKI-3-CERTIFICATE_INVALID.

IOS XE does not normalize different URL formats (IP vs. FQDN) as equivalent, even when both return identical CRL content for the same issuer.

Related Content

- Cisco Technical Support & Downloads