CDP URL이 여러 CRL 다운로드 URL과 일치하지 않아 IOS XE 인증서 유효성 검사 실패 해결

목차

문제

DMVPN(Dynamic Multipoint VPN) 허브 장치에 추가 CRL 다운로드 URL 위치가 추가되면 IKE 협상 실패로 인해 일부 스포크 터널이 설정되지 못하고 허브가 다음 오류를 로깅합니다.

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

인증서 체인 검증이 성공하고 CRL이 성공적으로 다운로드되더라도 폐기 확인에 간헐적으로 실패합니다.

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

이 문제는 DMVPN 허브 라우터가 동일한 CRL 파일을 가리키는 여러 CRL(Certificate Revocation List) 다운로드 URL 위치를 사용할 때 발생합니다. CRL 다운로드 위치에는 IP 기반 및 FQDN 기반 URL이 모두 포함되어 있지만 스포크 라우터에 발급된 인증서는 CDP(CRL 배포 지점)에만 FQDN 기반 URL이 있습니다.

환경

- 인증서 기반 IKE 인증을 사용하여 IPsec에 대해 구성된 IOS® XE 소프트웨어를 실행하는 Cisco 디바이스
- 동일한 CRL 파일을 호스팅하는 IP 기반 및 FQDN 기반 URL을 모두 포함하는 여러 CRL 다운로드 위치.

- 피어 디바이스에 발급된 인증서는 CDP에 하나의 URL만 있습니다.
- 인증서 해지 검사를 적용하는 동안 인증서 기반 인증을 사용하는 IPsec 터널 컨피그레이션입니다.

해결

CRL 검증 중에 정확한 URL 일치를 보장하기 위해 PKI 환경 전체에서 단일 표준 CDP URL을 표준화하는 작업이 해결됩니다.

권장 구현 단계

1. 허브 컨피그레이션에서 IP 기반 CRL 다운로드 URL을 제거합니다. 해당 IP 기반 CRL URL이 인증서 CDP의 일부가 아닌 경우

```
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. 스포크 인증서의 CDP와 일치하는 FQDN 기반 CRL 다운로드 URL만 구성합니다

```
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. 일관된 CDP URL을 사용하도록 발급 CA 템플릿 업데이트

발급 CA 템플릿이 FQDN 기반 CDP URL만 새로 발급된 인증서에 스탬프하도록 합니다.

4. 허브 및 스포크 인증서 재등록(새 CDP URL로 변경하는 경우)

새 CDP URL을 구현하는 경우 새 CDP URL을 게시하도록 발급 CA를 변경하고 새 URL을 전달하기 위해 허브 및 스포크 인증서를 모두 재등록합니다.

이중화 구현

예를 들어 CRL 제공자 리던던시의 경우, 호스팅 디바이스의 장애로부터 보호하기 위해 동일한 CRL이 다른 URL 위치에 게시되도록 하려면 다음을 사용하여 단일 FQDN 뒤에 백엔드 리던던시를 구현합니다.

- DNS 장애 조치
- 로드 밸런서
- 이중화 CRL 인프라

IOS XE에서는 동일한 CRL 파일을 참조하더라도 호스트 이름/IP가 서로 다른 CDP로 간주하므로 호스트 이름/IP가 서로 다른 여러 CDP를 사용하지 마십시오.

확인

변경 사항을 구현한 후 CRL 캐싱 및 터널 설정을 확인합니다.

```
show crypto pki crl
```

IKEv2 세션이 성공적으로 설정되었는지 확인합니다.

```
show crypto session details
```

원인

이 문제는 CRL 검증 중에 IOS XE와 정확한 CDP URL 일치 동작으로 인해 발생합니다. Revocation-check crl이 활성화된 피어 인증서의 유효성을 검사할 때 IOS XE는 유효성 검사 중인 인증서에 포함된 CDP URL과 허브의 구문 분석된 CRL 캐시에 저장된 CRL과 연결된 CDP URL 간의 정확한 문자열 일치를 수행합니다.

이 실패 순서는 다음과 같습니다.

1. 허브는 IP 기반 CDP URL을 사용하여 CRL을 성공적으로 다운로드하고 해당 URL 아래에 내부적으로 캐시합니다.
2. 스포크 인증서는 CDP에서 FQDN 기반 URL을 참조합니다.
3. 해지 검증 중에 IOS XE는 FQDN URL과 일치하는 캐시된 CRL을 검색합니다.
4. IOS XE는 IP 기반 및 FQDN 기반 URL을 서로 다른 CDP로 처리하기 때문에 정확한 일치 항목을 찾을 수 없습니다.
5. Router는 폐기 상태 = 2인 "No CRL found with matching CDP"를 반환합니다.
6. %PKI-3-CERTIFICATE_INVALID로 인해 인증서 유효성 검사가 실패했습니다.

IOS XE는 서로 다른 URL 형식(IP 대 FQDN)을 동일한 발급자에 대해 동일한 CRL 콘텐츠를 반환하는 경우에도 동일하게 표준화하지 않습니다.

관련 콘텐츠

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.