Resolver errores de validación de certificados de IOS XE debido a una discrepancia de URL de CDP con URL de descarga de CRL múltiple

Contenido

Problema

Después de agregar ubicaciones URL de descarga de CRL adicionales a un dispositivo hub de VPN multipunto dinámica (DMVPN), algunos túneles radiales no se pueden establecer debido a un error de negociación IKE y el hub registró este error:

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

Aunque la validación de la cadena de certificados se realiza correctamente y las CRL se descargan correctamente, la comprobación de revocación falla intermitentemente con:

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

Este problema se produce cuando el router hub DMVPN utiliza varias ubicaciones de URL de descarga de la lista de revocación de certificados (CRL) que apuntan al mismo archivo CRL. Las ubicaciones de descarga de CRL incluyen direcciones URL basadas en IP y FQDN, mientras que el certificado emitido para los enrutadores de radio solo tiene la dirección URL basada en FQDN en su punto de distribución de CRL (CDP).

Entorno

- Dispositivos Cisco que ejecutan el software IOS® XE configurado para IPsec mediante autenticación IKE basada en certificados.

- Varias ubicaciones de descarga de CRL con direcciones URL basadas en IP y FQDN que alojan los mismos archivos CRL.
- El certificado emitido a los dispositivos pares sólo tiene una URL en su CDP.
- Configuración de túnel IPsec mediante autenticación basada en certificados mientras se aplica la comprobación de revocación de certificados.

Resolución

La resolución implica la estandarización de una única URL CDP canónica en el entorno PKI para garantizar la coincidencia exacta de URL durante la validación de CRL.

Pasos de implementación recomendados

1. Elimine las URL de descarga de CRL basadas en IP de la configuración del hub, si dichas URL de CRL basadas en IP no forman parte de la CDP del certificado

```
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 solo URL de descarga de CRL basadas en FQDN que coincidan con el CDP en los certificados radiales

```
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. Actualizar plantillas de CA emisoras para utilizar URL CDP coherentes

Asegúrese de que las plantillas de CA emisoras estampen solo la URL CDP basada en FQDN en los certificados recién emitidos.

4. Vuelva a inscribir los certificados radiales y de concentrador (si cambia a la nueva URL CDP)

Si implementa una nueva URL CDP, cambie la CA emisora para publicar la nueva URL CDP y vuelva a inscribir los certificados hub y spoke para transmitir la nueva URL.

Implementación de redundancia

Para que la redundancia del proveedor de CRL, por ejemplo, tenga la misma CRL publicada en diferentes ubicaciones de URL para protegerse contra fallos en los dispositivos de alojamiento, implemente la redundancia de back-end detrás de un único FQDN mediante:

- falla de DNS
- Equilibrador de carga
- Infraestructura de CRL redundante

No utilice varios CDP con nombres de host/IP diferentes, ya que IOS XE los trata como CDP diferentes, incluso si hacen referencia al mismo archivo CRL.

Verificación

Después de implementar los cambios, verifique el almacenamiento en caché de CRL y el establecimiento de túnel:

```
show crypto pki crl
```

Confirme que la sesión IKEv2 se establece correctamente:

```
show crypto session details
```

Causa

El problema es causado por el comportamiento de coincidencia exacta de URL CDP de IOS XE durante la validación de CRL. Al validar un certificado de peer con la CRL de comprobación de revocación habilitada, IOS XE realiza una coincidencia de cadena exacta entre la URL CDP incrustada en el certificado que se valida y la URL CDP asociada con la CRL almacenada en la caché de CRL analizada del hub.

Esta secuencia de falla ocurre:

1. El concentrador descarga correctamente la CRL mediante una URL CDP basada en IP y la almacena en caché internamente bajo dicha URL.
2. Los certificados radiales hacen referencia a la URL basada en FQDN en su CDP.
3. Durante la validación de revocación, IOS XE busca una CRL en caché que coincida con la URL FQDN.
4. No se encuentra ninguna coincidencia exacta porque IOS XE trata las URL basadas en IP y FQDN como CDP diferentes.
5. El router devuelve "No se encontró ninguna CRL con el CDP coincidente" con el estado de revocación = 2.
6. Error en la validación del certificado con %PKI-3-CERTIFICATE_INVALID.

IOS XE no normaliza diferentes formatos de URL (IP frente a FQDN) como equivalentes, incluso cuando ambos devuelven contenido de CRL idéntico para el mismo emisor.

Contenido relacionado

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).