Résoudre les échecs de validation de certificat IOS XE dus à une non-correspondance d'URL CDP avec plusieurs URL de téléchargement CRL

Table des matières

Problème

Après l'ajout d'emplacements d'URL de téléchargement CRL supplémentaires à un périphérique concentrateur DMVPN (Dynamic Multipoint VPN), certains tunnels en étoile ne parviennent pas à s'établir en raison d'un échec de négociation IKE et le concentrateur enregistre cette erreur :

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

Bien que la validation de la chaîne de certificats réussisse et que les LCR soient téléchargées, la vérification de révocation échoue par intermittence avec :

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

Ce problème se produit lorsque le routeur concentrateur DMVPN utilise plusieurs emplacements d'URL de téléchargement de liste de révocation de certificats (CRL) pointant vers le même fichier CRL. Les emplacements de téléchargement de la liste de révocation de certificats incluent des URL basées sur IP et sur FQDN, tandis que le certificat délivré aux routeurs en étoile ne contient que l'URL basée sur FQDN dans son point de distribution de liste de révocation de certificats (CDP).

Environnement

- Périphériques Cisco exécutant le logiciel IOS® XE configuré pour IPsec à l'aide de l'authentification IKE basée sur certificat.
- Plusieurs emplacements de téléchargement de listes de révocation de certificats avec des URL basées sur IP et sur FQDN hébergeant les mêmes fichiers de listes de révocation de certificats.
- Le certificat délivré aux périphériques homologues ne contient qu'une seule URL dans son CDP.
- Configuration de tunnel IPsec utilisant l'authentification basée sur certificat lors de l'application du contrôle de révocation de certificat.

Résolution

La résolution implique la standardisation sur une URL CDP canonique unique dans l'environnement PKI afin de garantir une correspondance exacte des URL lors de la validation CRL.

Étapes de mise en oeuvre recommandées

1. Supprimez les URL de téléchargement CRL basées sur IP de la configuration du concentrateur, si ces URL CRL basées sur IP ne font pas partie du CDP du certificat

```
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. Configurez uniquement les URL de téléchargement de liste de révocation de certificats basées sur le nom de domaine complet qui correspondent au CDP dans les certificats satellite

```
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. Mettre à jour les modèles d'autorité de certification pour utiliser des URL CDP cohérentes

Assurez-vous que les modèles d’autorité de certification qui émettent marquent uniquement l’URL CDP basée sur le nom de domaine complet dans les certificats nouvellement émis.

4. Réinscrire les certificats Hub and Spoke (si vous passez à la nouvelle URL CDP)

Si vous implémentez une nouvelle URL CDP, modifiez l'autorité de certification émettrice pour publier la nouvelle URL CDP et réinscrivez les certificats Hub et Spoke pour transporter la nouvelle URL.

Implémentation de redondance

Par exemple, pour que la même liste de révocation de certificats soit publiée à différents emplacements d'URL afin de se protéger contre les défaillances sur les périphériques d'hébergement, implémentez la redondance du back-end derrière un seul nom de domaine complet à l'aide de :

- Basculement DNS
- Équilibreur de charge
- Infrastructure CRL redondante

N'utilisez pas plusieurs CDP avec des noms d'hôte/IP différents, car IOS XE les traite comme des CDP différents même s'ils font référence au même fichier CRL.

Vérification

Après avoir implémenté les modifications, vérifiez la mise en cache CRL et l'établissement du tunnel :

```
show crypto pki crl
```

Vérifiez que la session IKEv2 s'établit correctement :

```
show crypto session details
```

Motif

Le problème est causé par le comportement de correspondance exacte des URL CDP d'IOS XE lors de la validation de la liste de révocation de certificats. Lors de la validation d'un certificat homologue avec la commande revocation-check crl activée, IOS XE effectue une correspondance de chaîne exacte entre l'URL CDP incorporée dans le certificat en cours de validation et l'URL CDP associée à la liste de révocation de certificats stockée dans le cache de liste de révocation de certificats analysé du concentrateur.

Cette séquence de défaillance se produit :

1. Le concentrateur télécharge correctement la liste de révocation de certificats à l'aide de l'URL CDP IP et la met en cache en interne sous cette URL.
2. Les certificats satellite font référence à l'URL basée sur le nom de domaine complet dans son CDP.
3. Lors de la validation de la révocation, IOS XE recherche une liste de révocation de certificats mise en cache correspondant à l’URL FQDN.
4. Aucune correspondance exacte n'a été trouvée, car IOS XE traite les URL basées sur IP et les URL basées sur FQDN comme des CDP différents.
5. Le routeur renvoie « Aucune liste de révocation de certificats trouvée avec CDP correspondant » avec l'état de révocation = 2.
6. La validation du certificat a échoué avec %PKI-3-CERTIFICATE_INVALID.

IOS XE ne normalise pas différents formats d'URL (IP et FQDN) comme équivalents, même si les deux renvoient un contenu CRL identique pour le même émetteur.

Autres informations utiles

- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.