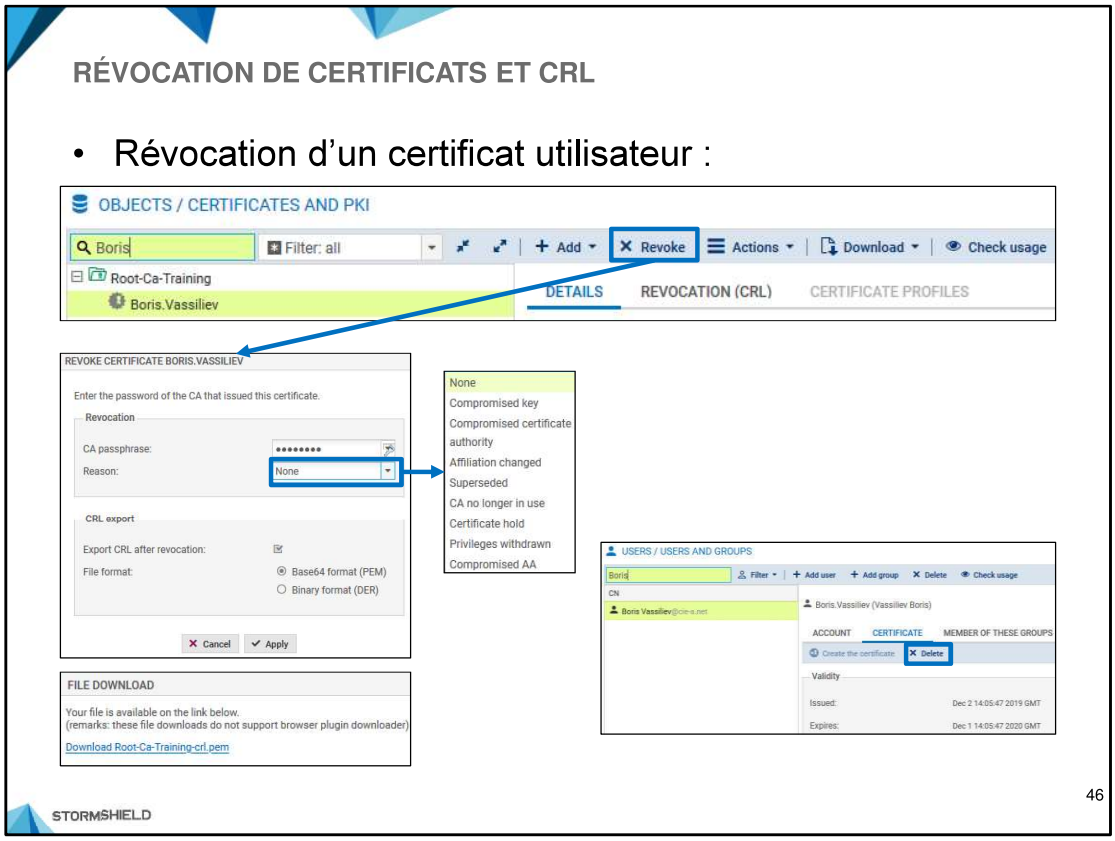
Programme du module

- ✔ Qu'est-ce que la cryptographie ?
- ✔ Eléments de cryptographie
- ✔ Infrastructures à clés publiques
- ✔ PKI Stormshield Network
- ✔ Création d'une autorité de certification
- ✔ Création d'une identité serveur
- ✔ Création d'une identité utilisateur
- ✔ Gestion des identités et certificats
- ➔ Révocation de certificats et CRL

  Lab - PKI



Révocation d'un certificat utilisateur

La révocation d'un certificat peut être nécessaire pour les raisons suivantes :

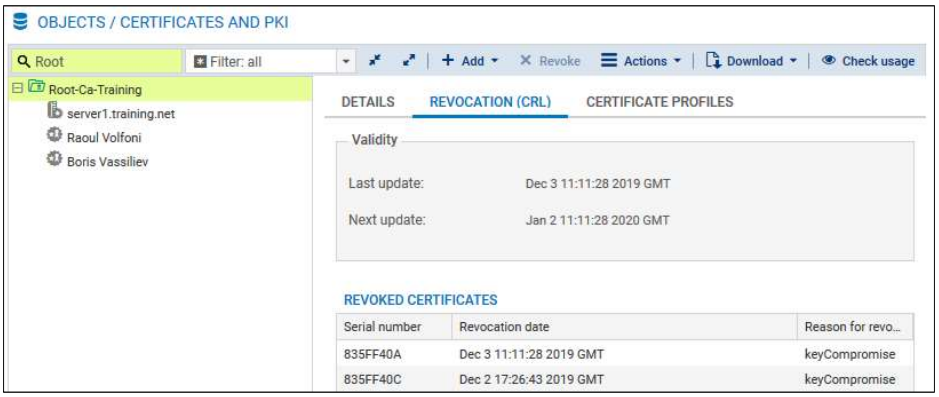
- la clé privée de l'utilisateur a été perdue ou volée,
- l'utilisateur change de fonction (son Unité d'Organisation (OU) est modifiée par exemple),
- l'identité a été renouvelée (l'ancien certificat n'est plus valide),
- Autres…

Révoquer le certificat

1. Mettez l'utilisateur souhaité en surbrillance,
2. Cliquez sur le menu **Révoquer**,
3. Tapez le mot de passe de la CA et choisissez la raison de la révocation,
4. Téléchargez la CRL (ré)générée et signée par la CA dès la fin de la révocation,
5. Si une copie du certificat utilisateur est stockée dans l'annuaire LDAP, cliquez sur le bouton **Supprimer**.

RÉVOCATION DE CERTIFICATS ET CRL

- Liste de révocation des certificats



47

STORMSHIELD

Liste de Révocation de Certificats

La CRL contient la liste des numéros de série des certificats révoqués.
La CRL est signée par la CA et possède également une période de validité (de un mois par défaut).

L'administrateur a la responsabilité de diffuser et publier la CRL sur les points de distribution renseignés lors de la création de l'Autorité.

ATTENTION : cette liste est vérifiée dès lors qu'elle est présente sur le firewall.
ELLE DOIT TOUJOURS ÊTRE EN COURS DE VALIDITÉ.

Si la période de validité de la CRL est expirée, la vérification des certificats révoqués n'est plus valable, l'ensemble des certificats issus de la CA correspondante ne peuvent plus être considérés comme valides.

STORMSHIELD

Maintien de la CRL d'une CA externe

Lorsque le certificat d'une CA externe est importé sur le firewall, il est possible d'ajouter une liste de CRLDP sur lesquels la présence d'une nouvelle CRL est vérifiée toutes les 24 heures.

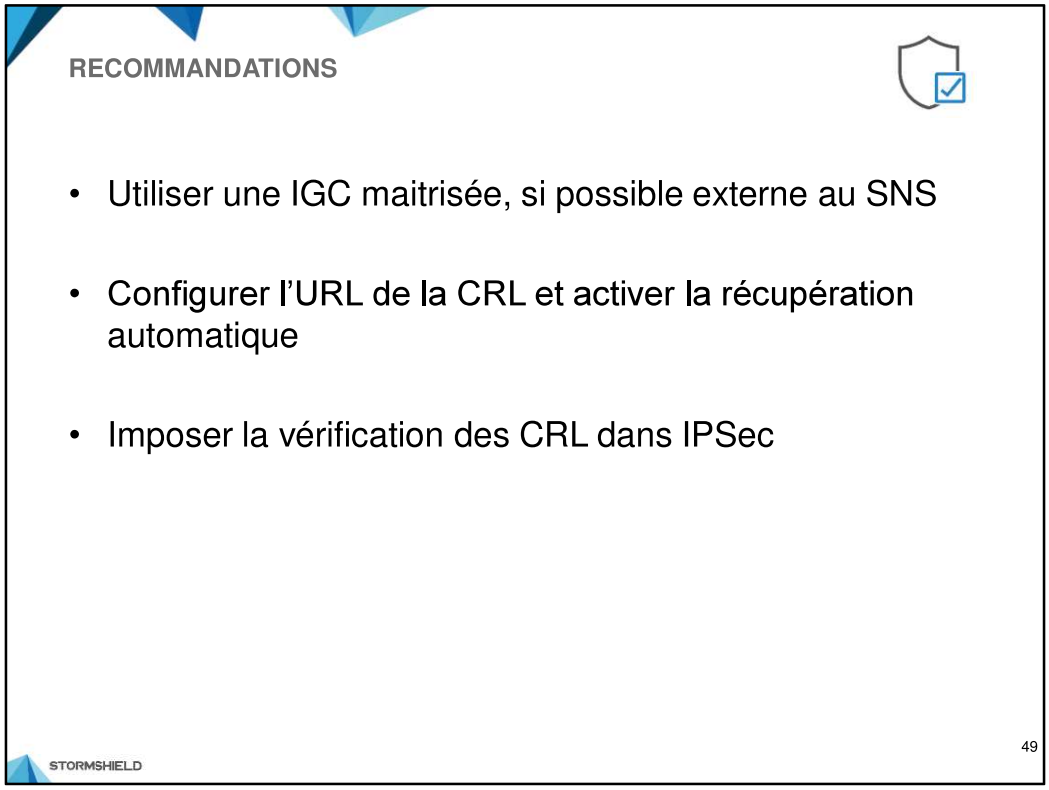
Pour assurer cette vérification, Il est impératif :

- De créer l'objet correspondant au nom d'hôte mentionné dans l'URL saisie,
- Que le nom du fichier de CRL géré par l'administrateur de la CA externe soit identique à celui renseigné dans l'URL.

La vérification s'effectue uniquement sur les URL saisies sur le firewall, et non sur les éventuels CRLDP présents dans le certificat de la CA externe.

NOTE

Le démon VPN IPSec charon utilisé par le firewall Stormshield a la possibilité d'effectuer dynamiquement une requête avec le protocole OCSP (Online Certificate Status Protocol) vers le serveur hébergeant la CRL, au lieu de devoir télécharger le fichier correspondant.



Il est recommandé d'utiliser une IGC (Infrastructure de Gestion de Clés ou PKI) externe au SNS. Ainsi en cas de compromission de l'équipement, seules les clés utilisées pour le fonctionnement de celui-ci sont compromises. De plus, cela permet d'utiliser des clefs basées sur les courbes elliptiques.

Il est recommandé de configurer les points de récupération de la CRL pour chaque CA. Sans cela les certificats révoqués ne seront pas connus du SNS. La récupération automatique se configure dans **Configuration > System > Configuration > Configuration générale** dans la zone **Paramètres cryptographiques**.

Par défaut IPSec ne vérifie pas la révocation des certificats. Pour imposer la vérification des CRL pour le profil 1, il faut utiliser les commandes NSRPC suivantes :

```
config ipsec update slot=01 CRLrequired=1
config ipsec activate
```

Faites attention à ce que la CRL soit bien bien accessible lors de l'établissement de la connexion.