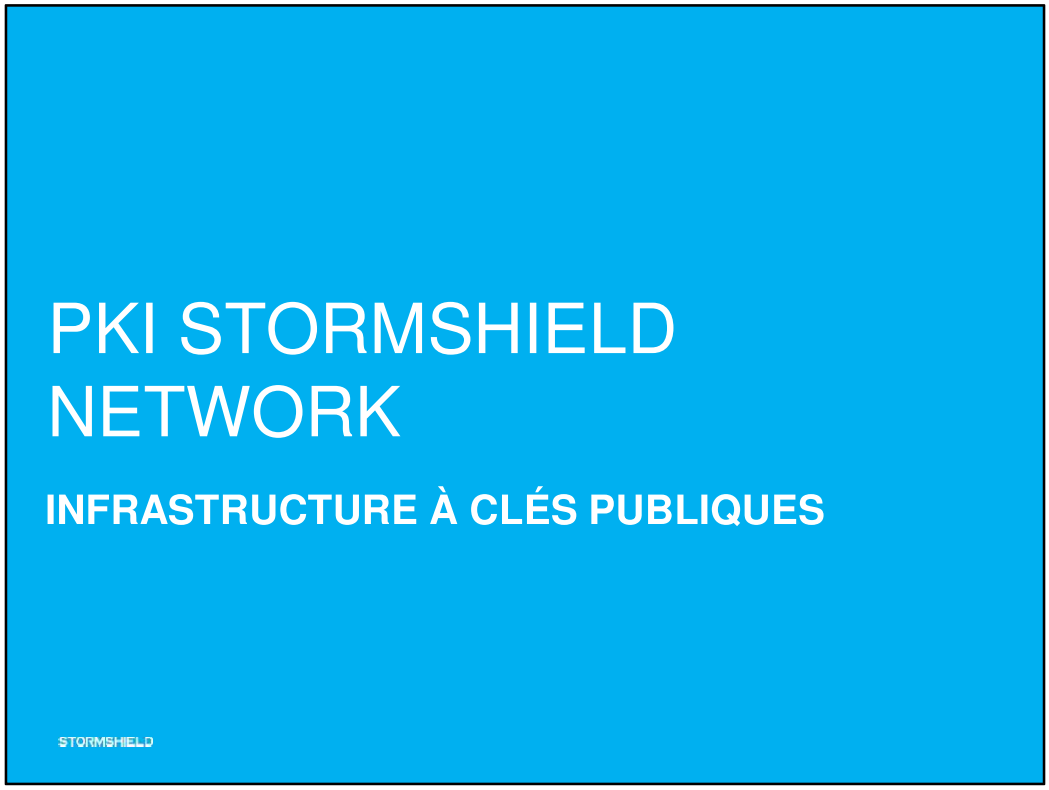
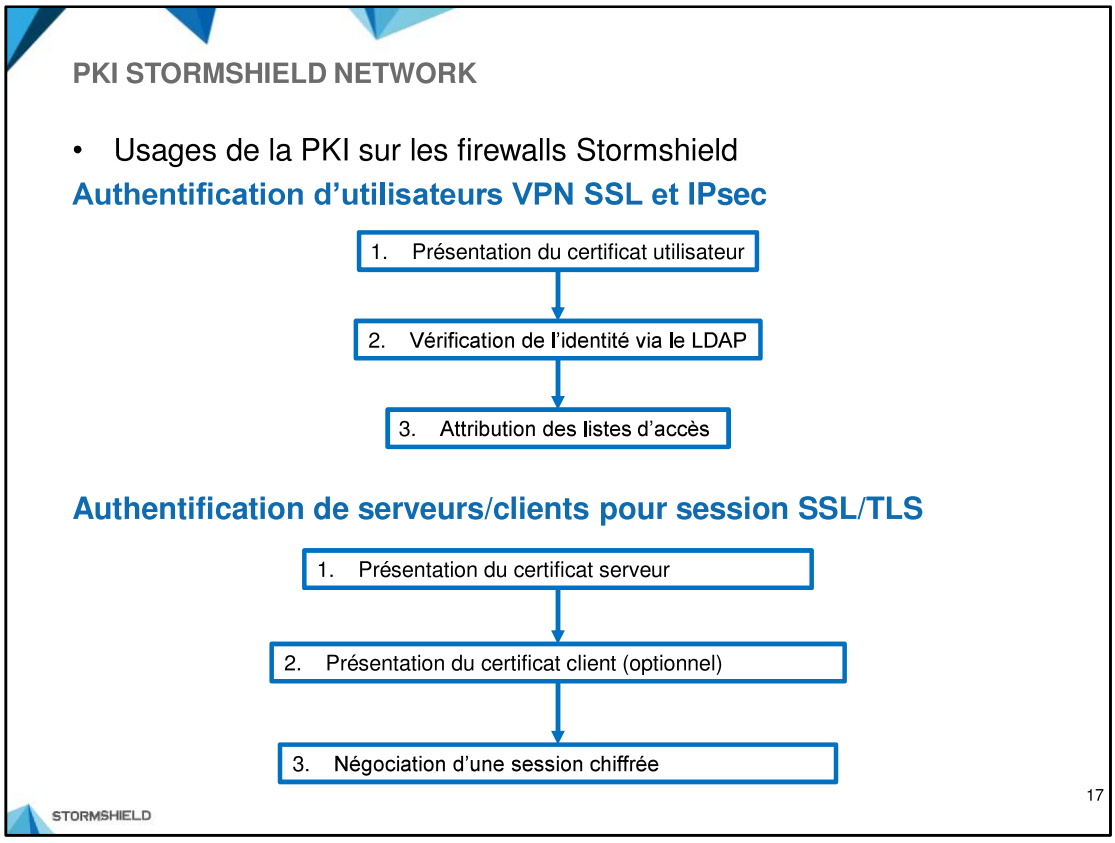


Programme du module

- ✔ 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



PKI Stormshield Network

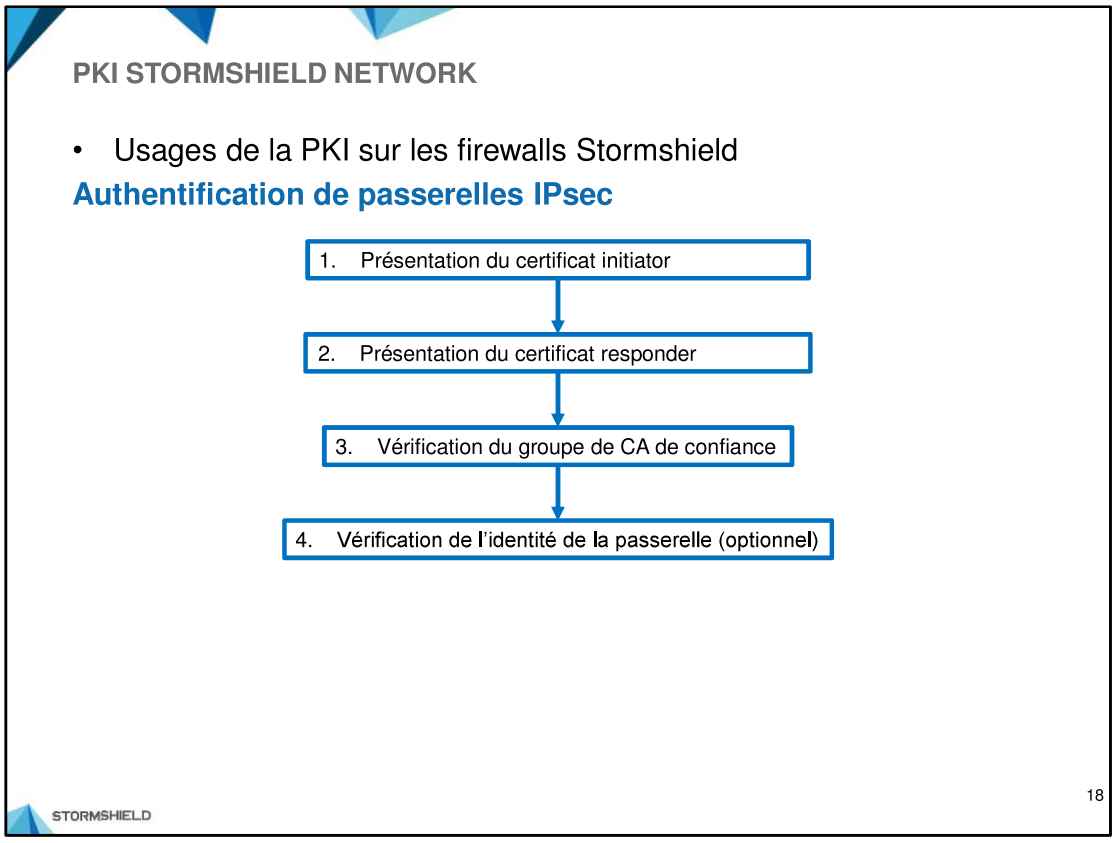
Les firewalls Stormshield intègrent les fonctions permettant la gestion des certificats, et ce, sur l'ensemble des produits SNS de la gamme.

Authentification d'utilisateurs

1. L'utilisateur mobile, ou l'administrateur de l'interface web, souhaitant s'authentifier auprès du firewall présente son certificat utilisateur, soit par son navigateur web, soit par son client VPN IPsec,
2. Le firewall vérifie la validité du certificat et contrôle l'identité de l'utilisateur sur le serveur LDAP,
3. Les politiques d'accès attachées à cet utilisateur peuvent alors lui être appliquées, pour permettre l'accès aux ressources réseau internes.

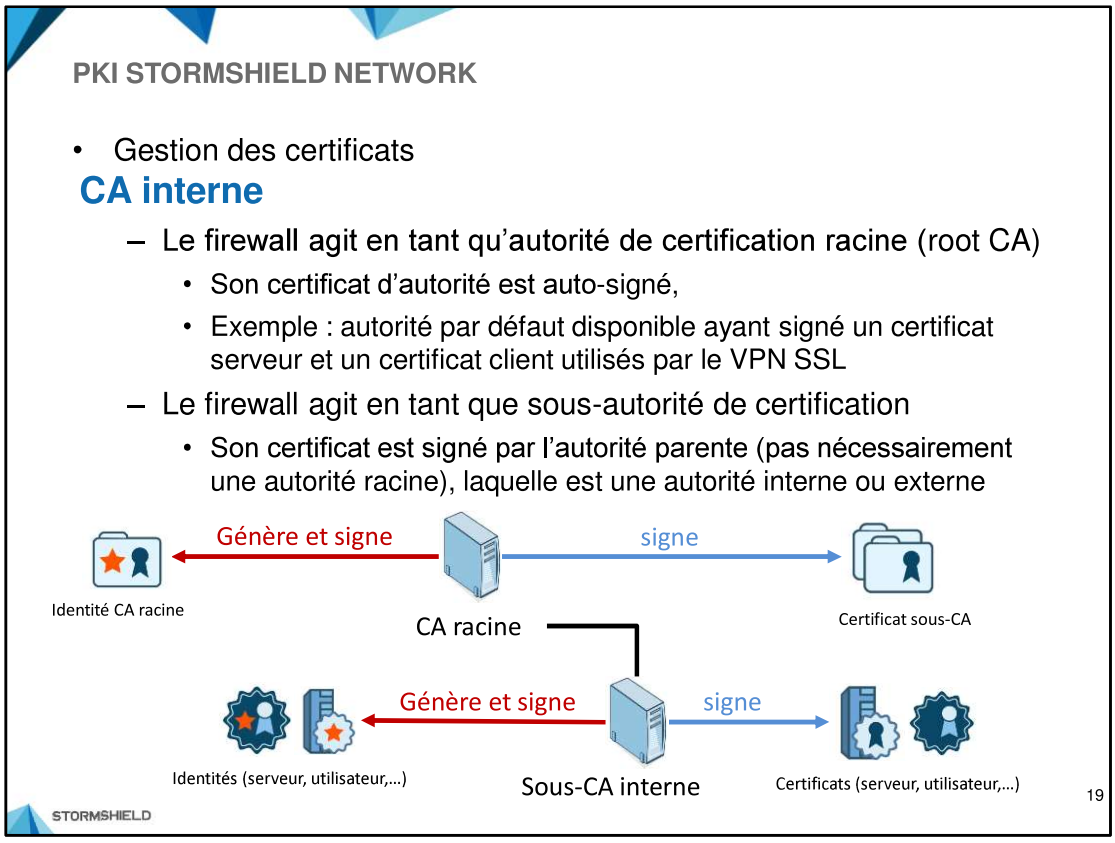
Authentification de serveurs (et / ou de clients)

1. Le serveur, lors de l'initialisation d'une session, présente son certificat serveur au client, lequel vérifie sa validité,
2. Éventuellement, le client présente son certificat client au serveur, lequel vérifie sa validité. Lorsque cette étape est présente, il s'agit d'une session avec authentification mutuelle (c'est le cas par exemple d'une session TCP/TLS entre le firewall client et le serveur Syslog Stormshield Visibility Center),
3. Après l'authentification, le client et le serveur négocient une clé de session.



Authentification de passerelles IPSec

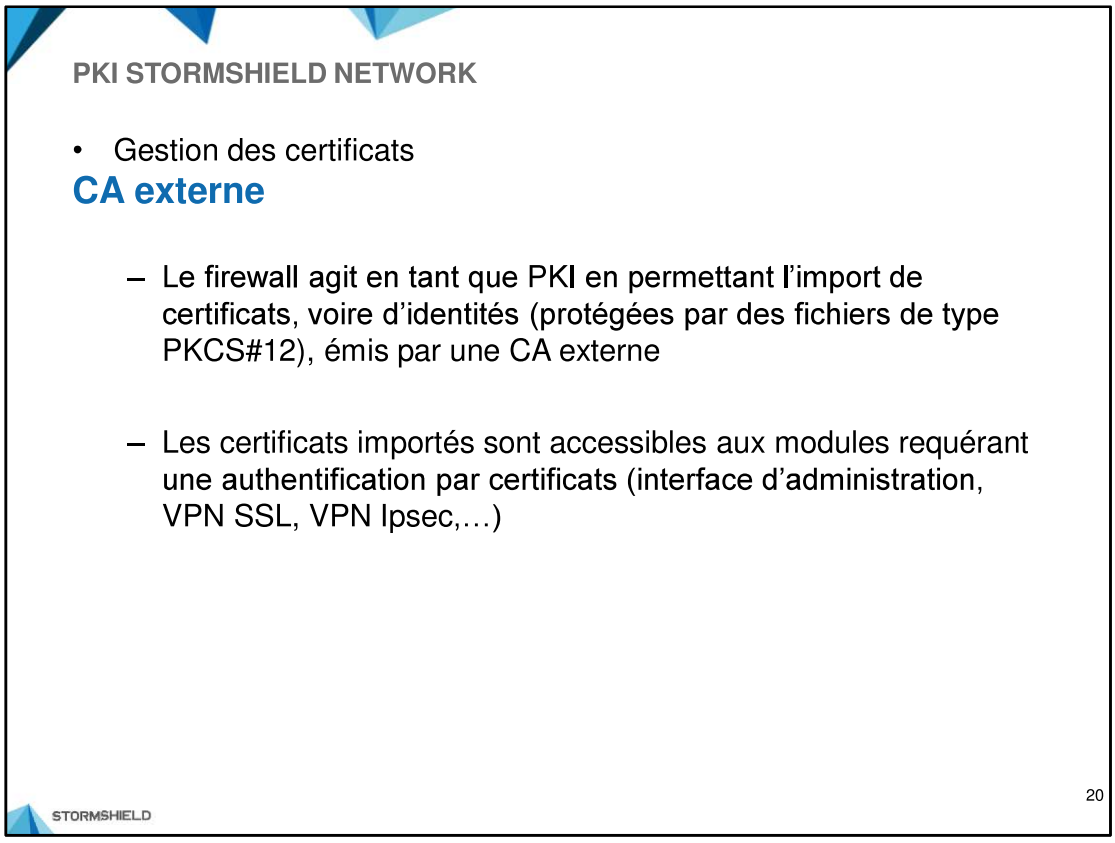
1. Lors de la phase d'établissement du tunnel, le firewall qui initie le tunnel (Initiator) présente son certificat à la passerelle distante, laquelle vérifie sa validité,
2. Le firewall qui répond (Responder) présente son certificat à la passerelle distante, laquelle vérifie sa validité,
3. Outre les vérifications effectuées sur la validité des certificats présentés (intégrité, signature numérique, période de validité,...), le certificat de l'autorité de certification ayant signé le certificat de la passerelle distante doit appartenir au groupe de confiance de CA, c'est-à-dire aux autorités de certification acceptées dans la politique VPN Ipsec,
4. La vérification de l'identité de la passerelle distante permet de garantir que le tunnel est monté avec la passerelle identifiée par le certificat, ce point optionnel ne peut être défini qu'en CLI.



CA interne

Cette fonctionnalité de gestion d'une infrastructure à clés publiques permet de répondre à un grand nombre de cas d'usage :

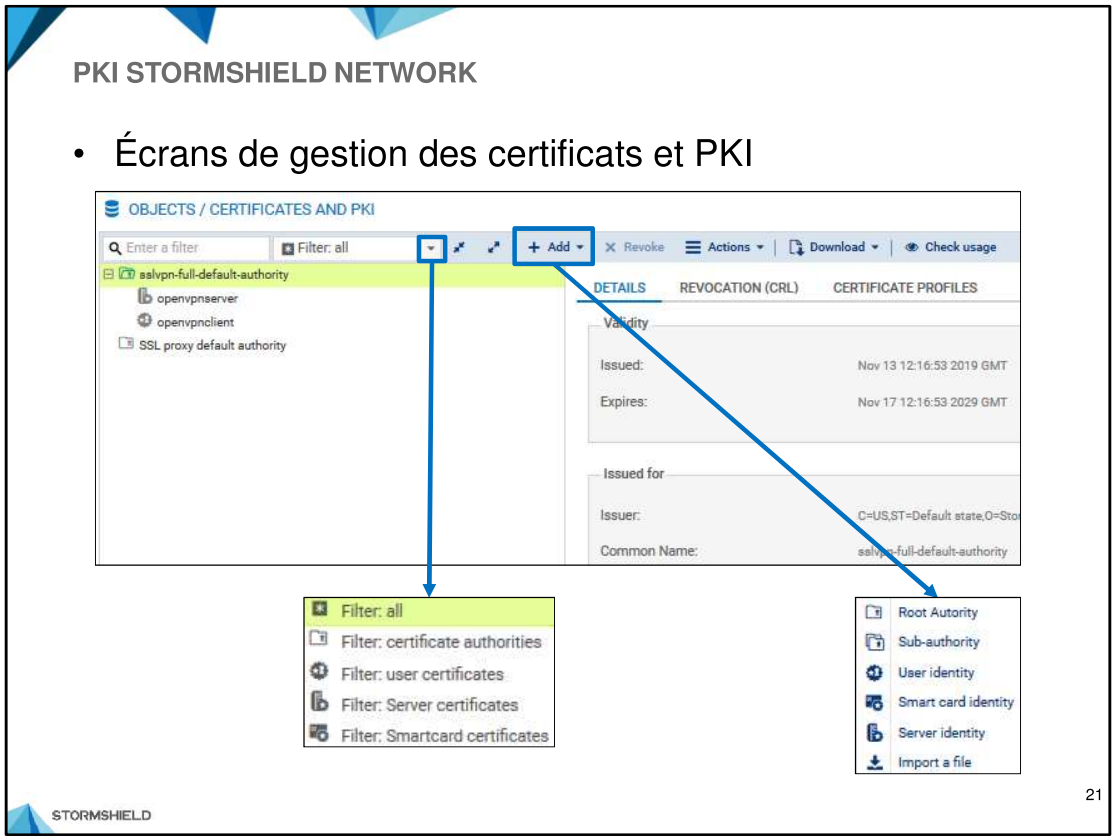
- **Autorité de certification racine :** Le boîtier SNS permet de définir les chaînes de confiance nécessaires à une authentification par certificat. Des autorités par défaut sont disponibles pour signer les certificats utilisés par le proxy SSL ou livrer les certificats nécessaires au fonctionnement du VPN SSL.
  Les fonctions proposées par le boitier SNS permettent de répondre pleinement au rôle d'autorité de certification (création de certificat de différentes natures, signature de CSR, révocation de certificat et gestion de CRL).
- **Sous-autorité de certification :** il est possible de définir un boitier SNS comme étant une sous-autorité de certification d'une CA parente. Une fois que le certificat de la sous-autorité est signé par l'autorité parente et importé dans le boîtier (dans le cas d'une CA externe), cela permet d'organiser plus finement la répartition et la distribution des identités, par usages ou par entités d'une même entreprise.



CA externe

Dans le cadre d'usage d'une CA externe, les fonctionnalités proposées permettent essentiellement d'importer des certificats et de définir les relations de confiance pour divers usages :

- Import de certificats d'autorité de certification.
- Import de certificats d'équipements.
- Import de certificats et de clés privés d'équipements (fichiers .p12 protégés ou pas par mot de passe).



L'écran du module Certificats et PKI se divise en trois parties :

- En haut de l'écran, les différentes actions possibles sous forme d'une barre de recherche et de boutons.
- A gauche, la liste des autorités et des identités ou certificats.
- A droite, les détails concernant l'autorité ou le certificat sélectionné au préalable dans la liste de gauche, ainsi que les informations concernant la CRL et la configuration de la CA ou sous CA.

La barre de recherche

Si vous recherchez un certificat ou une CA existante en particulier, saisissez son nom. Le champ de recherche vous permet de lister tous les certificats et les CA dont le nom correspond aux mots clés saisis.

Exemple :

Si vous saisissez la lettre « a » dans la barre de recherche, la liste en dessous fera apparaître tous les certificats possédant un « a ».

La zone de filtre

Cette zone permet de choisir le type de certificat à afficher et de ne voir que les éléments qui vous intéressent. Un menu déroulant vous propose les choix suivants :

Tous	Affiche dans la liste de gauche, toutes les autorités et certificats préalablement créés.
Autorités	Affiche dans la liste de gauche, toutes les autorités et sous-autorités.
Certificats utilisateur	Affiche uniquement les certificats utilisateur et les CA dont ils dépendent.
Certificats serveur	Affiche seulement les certificats serveur et les CA dont ils dépendent.
Certificats Smartcard	Affiche uniquement les certificats Smartcard et les CA dont ils dépendent.

Les assistants de configuration

Cette zone permet de démarrer les assistants d'ajout d'éléments dans les objets Certificats et PKI :

Ajouter une autorité racine	Lance l'assistant permettant de créer une autorité de certification racine gérée par le firewall. Cette autorité peut être une sous-autorité d'une PKI externe.
Ajouter une sous-autorité	Lance l'assistant permettant de créer une autorité de certification dépendant d'une autre CA. L'autorité parente doit être gérée par le boitier.
Ajouter une identité utilisateur	Lance l'assistant permettant de créer une identité utilisateur dépendant d'une autorité de certification gérée par le boitier.
Ajouter une identité serveur	Lance l'assistant permettant de créer une identité serveur dépendant d'une autorité de certification gérée par le boitier.
Ajouter une identité Smartcard	Lance l'assistant permettant de créer une identité Smartcard dépendant d'une autorité de certification gérée par le boitier.
Importer un fichier	Le fichier importé peut être une identité, un certificat, une CRL.