



Gestion des certificats Stormshield (PKI)

ES-SAIDI NAUFAL

Sommaire

1. Présentation

- Rôle de la PKI et des certificats X.509
- Sécurisation et authentification des communications

2. Fonctionnalités

- Création de certificats et autorités (CA)
- Gestion des révocations
- Sécurisation VPN, HTTPS et services TLS

3. Accès au module

- CONFIGURATION > OBJETS > Certificats et PKI

4. Types de CA

- **CA interne** : création et gestion des certificats
- **CA externe** : import de certificats tiers

5. Création d'une CA

- Accès au menu puis **Ajouter > Autorité racine**
- Paramètres principaux : identité, mot de passe, durée, clé

6. Conclusion

- Authentification fiable et sécurité renforcée

GESTION DES CERTIFICATS SUR PARE-FEU STORMSHIELD (PKI)

PRESENTATION

Le pare-feu **Stormshield SNS** intègre une infrastructure à clés publiques (PKI) permettant la gestion des certificats numériques.

Cette **PKI** assure l'authentification sécurisée des utilisateurs, serveurs et équipements via des **certificats X.509**.

Elle permet notamment :

- 0. la création d'autorités de certification (CA),**
- **la génération d'identités utilisateur et serveur,**
- **la gestion des révocations,**
- **la sécurisation des accès (VPN, interface d'administration, services TLS).**

Accès au module **PKI** :

CONFIGURATION > OBJETS > Certificats et PKI

TYPES D'AUTORITES DE CERTIFICATION

CA INTERNE :

Le pare-feu agit comme autorité de certification locale. Il peut :

- 0. créer et signer des certificats,**
- **gérer les listes de révocation (CRL),**
- **jouer le rôle de CA racine ou de sous-autorité,**
- **servir de base de confiance pour VPN SSL/IPSec et authentification.**

Le certificat de la CA est auto-signé et contrôle toute la chaîne de confiance interne.

CA EXTERNE :

Le pare-feu peut importer :

- 0. des certificats signés par une autorité tierce,**
- **des fichiers PKCS#12 (.p12),**
- **des certificats d'équipements ou serveurs.**

Ces certificats sont utilisés pour :

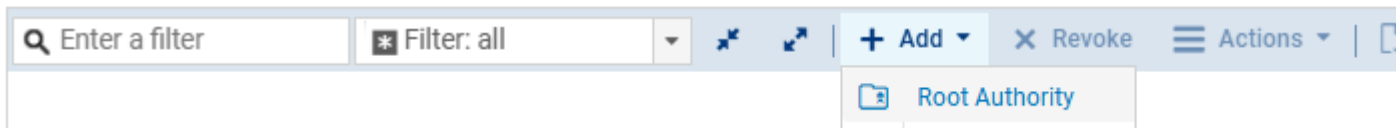
- 0. VPN IPSec / SSL**
- **HTTPS sécurisé**
- **authentification des équipements**

CREATION D'UNE AUTORITE DE CERTIFICATION

Procédure :

1. Menu : CONFIGURATION > OBJETS > Certificats et PKI
Cliquer sur **Ajouter > Autorité racine**

OBJECTS / CERTIFICATES AND PKI



Informations à renseigner :

0. **CN : nom de l'autorité (ex : CA_Stormshield)**
 - Organisation (O)
 - Unité d'organisation (OU)
 - Ville / Pays

Paramètres :

0. **Mot de passe de protection**
 - Durée de validité conseillée : 365 jours
 - Taille de clé : 2048 bits recommandée

L'autorité devient alors la racine de confiance pour la génération des certificats.

CONCLUSION:

La mise en place d'une **PKI** sur le pare-feu Stormshield permet de renforcer la sécurité du réseau en garantissant :

0. **l'identité des utilisateurs et équipements,**
 - l'intégrité des communications,
 - une authentification fiable et centralisée.