

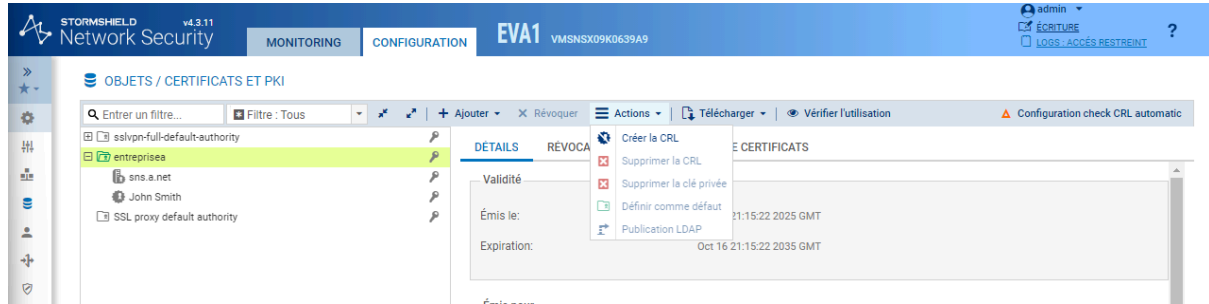
# Lab 13 – VPN IPsec Site à Site avec certificat

## Table des matières :

1. Configuration du serveur VPN.....	2
--------------------------------------	---

# 1. Configuration du serveur VPN

- Nous créons la CRL



- Nous attribuons comme mot de passe de la CA 123AZEqsdl et nous exportons au format .PEM
- Téléchargement de la CRL (fichier au format PEM) afin de l'importer ultérieurement sur le Firewall distant FwB

## TÉLÉCHARGEMENT DE FICHIER

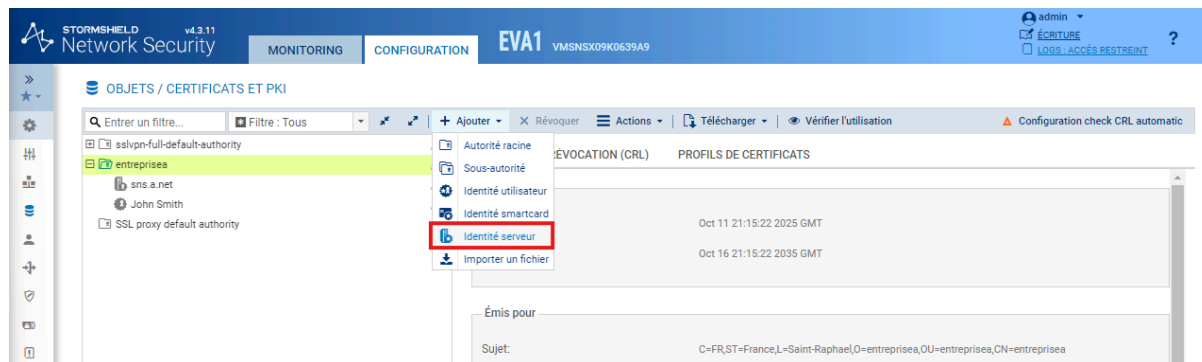
Le fichier est disponible via le lien ci-dessous.  
(Remarque : ces téléchargements ne supportent pas les extensions de téléchargement installées sur le navigateur)

[Télécharger entreprisea-crl.pem](#)

## Téléchargements

- entreprisea-crl (1).pem  
[Ouvrir un fichier](#)
- entreprisea-crl.pem  
[Ouvrir un fichier](#)

- Création du certificat du Firewall distant depuis l'autorité de certification (FwA)



The screenshot shows the Stormshield Network Security interface. The top navigation bar includes 'MONITORING' and 'CONFIGURATION' tabs, with 'EVA1' and 'VMSNSX09K0639A9' displayed. The main content area is titled 'OBJETS / CERTIFICATS ET PKI'. A tree view on the left shows a hierarchy: 'sslvpn-full-default-authority' > 'entreprisea' > 'sns.a.net' > 'John Smith'. A context menu is open over 'John Smith', with 'Identité serveur' highlighted in red. The right pane shows 'EVOCACTION (CRL)' and 'PROFILS DE CERTIFICATS' with a table of certificates:

Émis pour	Expiration
	Oct 11 21:15:22 2025 GMT
	Oct 16 21:15:22 2035 GMT

Below the table, the 'Sujet' field contains the value: 'C=FR,ST=France,L=Saint-Raphael,O=entreprisea,OU=entreprisea,CN=entreprisea'.

## CRÉER UNE IDENTITÉ SERVEUR

### OPTIONS DE L'IDENTITÉ - ASSISTANT DE CRÉATION



Nom de domaine qualifié (FQDN):

Identifiant:

✖ ANNULER


⏪ PRÉCÉDENT

⏩ SUIVANT

Mot de passe de la CA : 123AZEqsdl

CRÉER UNE IDENTITÉ SERVEUR

**OPTIONS DE L'IDENTITÉ - ASSISTANT DE CRÉATION**



Sélectionnez l'autorité parente

Autorité parente:

Mot de passe de la CA:

Attributs de l'autorité

Organisation (O):

Unité d'organisation (OU):

Ville (L):

État (ST):

Pays (C):

CRÉER UNE IDENTITÉ SERVEUR

**OPTIONS DE L'IDENTITÉ - ASSISTANT DE CRÉATION**



Validité (jours):

Type de clé:

Taille de clé (bits):

## CRÉER UNE IDENTITÉ SERVEUR

## AJOUT D'ALIAS - ASSISTANT DE CRÉATION



+ Ajouter   × Supprimer   ↑ Monter   ↓ Descendre

URI (address)

--

× ANNULER

« PRÉCÉDENT

» SUIVANT

## CRÉER UNE IDENTITÉ SERVEUR

## RÉSUMÉ

Terminez cet assistant afin de créer l'identité serveur ci-dessous

Nom:	sns.b.net
Identifiant:	sns.b.net
Autorité parente:	entreprisea
Organisation (O):	entreprisea
Unité d'organisation (OU):	entreprisea
Ville (L):	Saint-Raphael
État (ST):	France
Pays (C):	FR
Type de clé:	RSA
Taille de clé:	2048

Valide jusque Mon Oct 19 2026 12:07:09 GMT+0200 (heure d'été d'Europe centrale) soit 365 jours

✗ ANNULER

⏪ PRÉCÉDENT

✓ TERMINER

- Nous téléchargeons l'identité du site distant B (format P12) :

The screenshot shows the Stormshield management console. The main area is titled 'OBJETS / CERTIFICATS ET PKI'. A search bar at the top contains 'Entrer un filtre...' and a filter dropdown is set to 'Tous'. A list of objects is displayed, including 'sslvpn-full-default-authority', 'entreprisea', 'sns.a.net', 'John Smith', 'sns.b.net' (highlighted in green), and 'SSL proxy default authority'. A context menu is open over 'sns.b.net', showing options: '+ Ajouter', 'Vérifier l'utilisation', 'Télécharger', 'Actions', and 'Révoquer'. The 'Télécharger' option is expanded, showing sub-options: 'Certificat', 'Identité', and 'CRL'. The 'Identité' sub-option is further expanded, showing 'Au format PEM' and 'Au format P12', with the latter highlighted by a red box. On the right side, a 'DÉTAILS' panel is visible, showing fields for 'Validité', 'Émis le:', 'Expiration:', and 'Sujet:'.

- Nous y spécifions le mot de passe 123AZEqsdf!

ENTREZ UN MOT DE PASSE POUR PROTÉGER LE CERTIFICAT SNS.B.NET

Entrez le mot de passe:

Confirmer:

Excellent

Télécharger le certificat (P12) Annuler

## Téléchargements

sns.b.net.p12  
[Ouvrir un fichier](#)

- Nous ajoutons la CA dans les autorités de certification acceptées

### VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

#### AUTORITÉ DE CERTIFICATION ACCEPTÉES

+ Ajouter X Supprimer

CA ↑

entreprisea

- Nous modifions le correspondant IPsec (Site\_FW\_B) : certificat à présenter à B

### VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

Entrer un filtre... + Ajouter

Passerelles distantes (1)

Site\_fw\_B

Correspondants mobiles (1)

nomade\_entreprisea

#### SITE\_FW\_B

##### Général

Commentaire:

Passerelle distante: Fw\_B

Adresse locale: Any

Profil IKE: IKE\_Phase1

Version IKE: IKEv2

##### Identification

Méthode d'authentification: Certificat

Certificat: entreprisea.sns.a.net

Local ID: Saisir un identifiant (optionnel)

ID du correspondant: Saisir un identifiant (optionnel)

Clé pré-partagée (PSK):  Éditer

Configuration avancée

- Nous sélectionnons la politique de chiffrement et nous vérifions la présence du tunnel VPN

The screenshot shows the Stormshield Network Security v4.3.11 interface. The top navigation bar includes 'MONITORING' and 'CONFIGURATION' tabs, with 'EVA1' and 'VMSNSX09K0639A9' displayed. The user is logged in as 'admin'. The main content area is titled 'VPN / VPN IPSEC' and has sub-tabs for 'POLITIQUE DE CHIFFREMENT - TUNNELS', 'CORRESPONDANTS', 'IDENTIFICATION', and 'PROFILS DE CHIFFREMENT'. The 'POLITIQUE DE CHIFFREMENT - TUNNELS' tab is active, showing a table of VPN policies. The table has columns for 'Etat', 'Réseau local', 'Correspondant', 'Réseau distant', 'Profil de chiffrement', 'Keepalive', and 'Commentaire'. Two policies are listed: 'LAB 13 (contient 1 règles, de 2 à 2)' and 'VTI (contient 1 règles, de 4 à 4)'. The 'VTI' policy is highlighted in green and shows details: 'Network\_in' for local network, 'Site\_fw\_B' for correspondent, 'Lan\_in\_B' for remote network, and 'IKE\_Phase2' for encryption profile. The 'Keepalive' value is 30 and the comment is 'Originally created on 2025-0...'.

- Nous vérifions la présence des règles de filtrage pour un test ftp + ping (B vers A)

The screenshot shows the 'Règle Ipsec (contient 4 règles, de 4 à 7)' section. It displays a table of firewall rules. Two rules are visible: rule 4 and rule 5. Rule 4 is highlighted in green and has the following details: ID 4, status 'on', action 'passer', source 'Lan\_in\_B DMZ\_in\_B via Tunnel VPN IPsec', destination 'Network\_in Network\_dmz1', protocol 'Any', and service 'icmp (requête Echr)'. Rule 5 is also highlighted in green and has the following details: ID 5, status 'on', action 'passer', source 'Lan\_in\_B DMZ\_in\_B via Tunnel VPN IPsec', destination 'srv\_ftp\_priv srv\_web\_priv', protocol 'ftp http', and service 'IPSec'. The creation date for rule 4 is 'Créée le 2025-10-02 13:21:02, p...' and for rule 5 is 'Créée le 2025-10-02 13:40:06, p...'.