

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

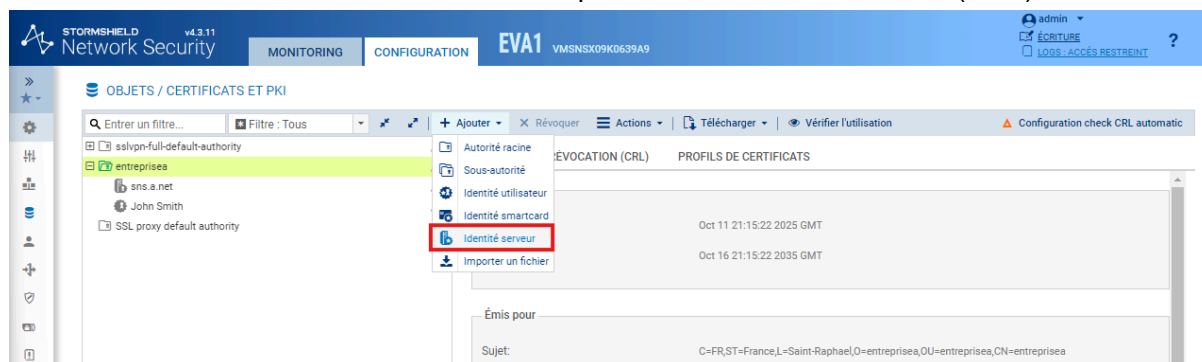
Le fichier est disponible via le lien ci-dessous.
(Remarque : ces téléchargements ne supportent pas les extensions de téléchargement installées sur le navigateur)

[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)



CRÉER UNE IDENTITÉ SERVEUR

OPTIONS DE L'IDENTITÉ - ASSISTANT DE CRÉATION



Nom de domaine qualifié (FQDN):

sns.b.net

Identifiant:

sns.b.net

✖ 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: entreprisea

Mot de passe de la CA:

Attributs de l'autorité

Organisation (O): entreprisea

Unité d'organisation (OU): entreprisea

Ville (L): Saint-Raphael

État (ST): France

Pays (C): France

✕ ANNULER << PRÉCÉDENT >> SUIVANT

CRÉER UNE IDENTITÉ SERVEUR

OPTIONS DE L'IDENTITÉ - ASSISTANT DE CRÉATION



Validité (jours): 365

Type de clé: RSA

Taille de clé (bits): 2048

✕ ANNULER << PRÉCÉDENT >> SUIVANT

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) :

OBJETS / CERTIFICATS ET PKI

Entrer un filtre... Filtre : Tous

+ Ajouter ✕ Révoquer

sslvpn-full-default-authority

entreprisea

sns.a.net

John Smith

sns.b.net

SSL proxy default authority

+ Ajouter

✓ Vérifier l'utilisation

📄 Télécharger

⋮ Actions

✕ Révoquer

Certificat

Identité

CRL

Au format PEM

Au format P12

Validité

Émis le:

Expiration:

Sujet:

- Nous y spécifions le mot de passe 123AZEqsds!

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 left sidebar contains various icons for navigation. The main content area is titled 'VPN / VPN IPSEC' and has tabs for 'POLITIQUE DE CHIFFREMENT - TUNNELS', 'CORRESPONDANTS', 'IDENTIFICATION', and 'PROFILS DE CHIFFREMENT'. The 'POLITIQUE DE CHIFFREMENT - TUNNELS' tab is active, showing a list of policies. The first policy is 'IPsec 01 (01)', which is highlighted. Below the list, there are sections for 'SITE À SITE (GATEWAY-GATEWAY)' and 'MOBILE - UTILISATEURS NOMADES'. The 'SITE À SITE (GATEWAY-GATEWAY)' section shows a table with columns: 'Etat', 'Réseau local', 'Correspondant', 'Réseau distant', 'Profil de chiffrement', 'Keepalive', and 'Commentaire'. The table contains two entries: 'LAB 13 (contient 1 règles, de 2 à 2)' and 'VTI (contient 1 règles, de 4 à 4)'. The 'LAB 13' entry is expanded, showing a table with columns: 'Réseau local', 'Correspondant', 'Réseau distant', 'Profil de chiffrement', 'Keepalive', and 'Commentaire'. The table contains one entry: '2' with 'on' status, 'Network_in' as the local network, 'Site_fw_B' as the corresponding network, 'Lan_in_B' as the remote network, 'IKE_Phase2' as the profile, '30' as the keepalive, and 'Originally created on 2025-0...' as the comment.

- 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 with columns: 'Id', 'Etat', 'Action', 'Réseau local', 'Réseau distant', 'Profil de chiffrement', 'Keepalive', and 'Commentaire'. The table contains two entries: '4' and '5'. The '4' entry is expanded, showing a table with columns: 'Réseau local', 'Réseau distant', 'Profil de chiffrement', 'Keepalive', and 'Commentaire'. The table contains one entry: '4' with 'on' status, 'passer' as the action, 'Lan_in_B' as the local network, 'DMZ_in_B' as the remote network, 'Network_in' as the profile, 'Any' as the keepalive, and 'icmp (requête Echr)' as the comment. The '5' entry is also expanded, showing a table with columns: 'Réseau local', 'Réseau distant', 'Profil de chiffrement', 'Keepalive', and 'Commentaire'. The table contains one entry: '5' with 'on' status, 'passer' as the action, 'Lan_in_B' as the local network, 'DMZ_in_B' as the remote network, 'Network_in' as the profile, 'Any' as the keepalive, and 'ftp http' as the comment.