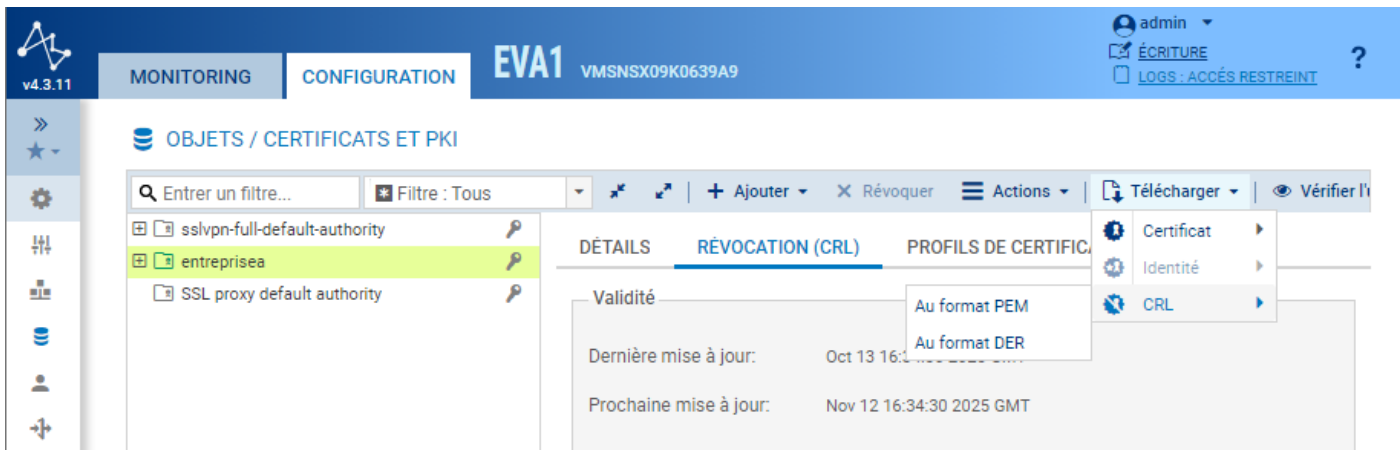


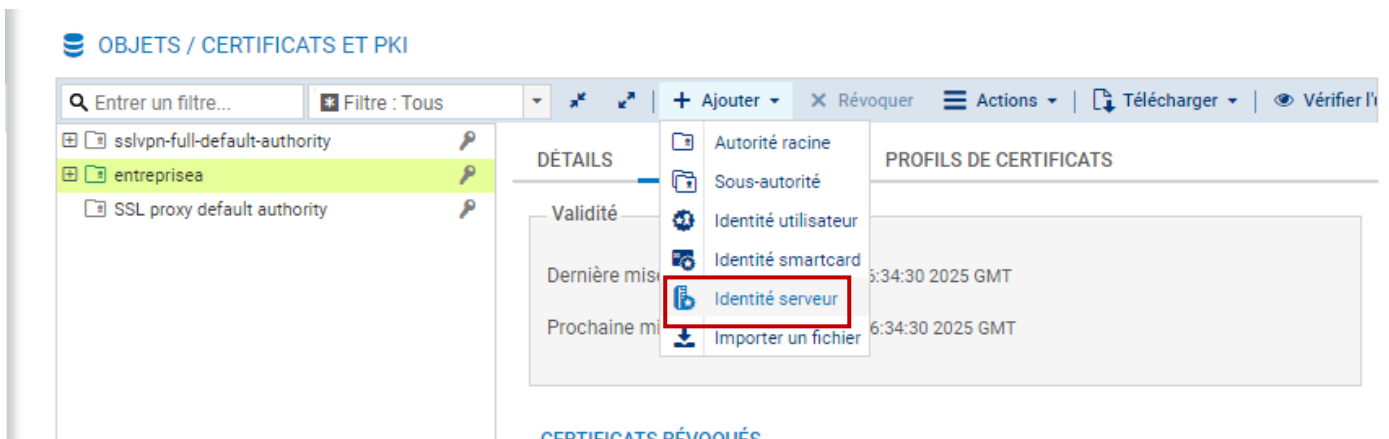
# Lab 13 – VPN IPsec Site à Site avec certificat

- Je télécharge la CRL afin de l'importer sur FwB :



The screenshot shows the Fortinet configuration interface for 'EVA1'. The 'OBJETS / CERTIFICATS ET PKI' section is open, and the 'entreprisea' object is selected. The 'RÉVOCATION (CRL)' tab is active, displaying details for the CRL, including its validity and update dates. A dropdown menu is open, showing options to download the CRL in PEM or DER format.

- Je crée le certificat du Firewall distant depuis l'autorité de certification :



The screenshot shows the Fortinet configuration interface for 'EVA1'. The 'OBJETS / CERTIFICATS ET PKI' section is open, and the 'entreprisea' object is selected. The 'PROFILS DE CERTIFICATS' tab is active, displaying details for the certificate profile, including its validity and update dates. A dropdown menu is open, showing options to create a new certificate profile, including 'Identité serveur'.

- Je renseigne sns.b.net :



The screenshot shows the Fortinet configuration interface for 'EVA1'. The 'CRÉER UNE IDENTITÉ SERVEUR' section is open, and the 'OPTIONS DE L'IDENTITÉ - ASSISTANT DE CRÉATION' is displayed. The 'Nom de domaine qualifié (FQDN)' and 'Identifiant' fields are both set to 'sns.b.net'. The 'Identifiant' field is highlighted with a red box.

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

➤ Je laisse par défaut :

OPTIONS DE L'IDENTITÉ - ASSISTANT DE CRÉATION



Validité (jours):

365

Type de clé:

RSA

Taille de clé (bits):

2048

✗ ANNULER

⏪ PRÉCÉDENT

⏩ SUIVANT

➤ Je ne renseigne pas d'URL :

## CRÉER UNE IDENTITÉ SERVEUR

### AJOUT D'ALIAS - ASSISTANT DE CRÉATION



<b>+ Ajouter</b> <b>X Supprimer</b> <b>↑ Monter</b> <b>↓ Descendre</b>
URI (address)

**X ANNULER**   **« PRÉCÉDENT**   **» SUIVANT**

➤ J'observe le résumé :

## CREER UNE IDENTITE 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 Tue Oct 13 2026 16:36:13 GMT+0200 (heure d'été d'Europe centrale) soit 365 jours

**X ANNULER**   **« PRÉCÉDENT**   **✓ TERMINER**

- J'exporte en .p12 les données de sécurité des sites distants :

OBJETS / CERTIFICATS ET PKI

Entrez un filtre... Filtre : Tous + Ajouter Révoquer Actions Télécharger Vérifier l'

sslvpn-full-default-authority  
entreprisea  
  sns.a.net  
  John Smith  
  sns.b.net  
SSL proxy default authority

DÉTAILS RÉVOCATION (CRL) PROFILS DE CERTIFICATS

Validité

Émis le: Oct 12 16:37:44 2025 GMT

Expiration: Oct 13 16:37:44 2026 GMT

- Je modifie le correspondant IPsec :

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

Entrez un filtre... Passerelles distantes (1) Site\_Fw\_B Correspondants mobiles (1) nomade\_entrepr...

SITE\_FW\_B

Général

Commentaire:

Passerelle distante: Fw\_B

Adresse locale: Any

Profil IKE: StrongEncryption

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

- Je sélectionne la politique de chiffrement :

POLITIQUE DE CHIFFREMENT - TUNNELS    CORRESPONDANTS    IDENTIFICATION    PROFILS DE CHIFFREMENT

IPsec 01 (01)    Actions    Deactivate policy

SITE À SITE (GATEWAY-GATEWAY)    MOBILE - UTILISATEURS NOMADES

Entrer un filtre...    Ajouter    Supprimer    Monter    Descendre    Couper    Copier    Coller    A

	Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffre...	Keepalive	Commentaire
1	on	Network_intern	Site_Fw_B	Lan_in_B	IPSECphase2Noma	30	Originally create...

➤ J'importe le certificat :

Ajouter    Révoquer    Actions    Télécharger    Vérifier l'utilisation

Choisissez l'élément à importer dans la barre de recherche pour filtrer la liste

- Autorité racine
- Sous-autorité
- Identité utilisateur
- Identité smartcard
- Identité serveur
- Importer un fichier**

➤ Je renseigne la bonne extension et le mot de passe du fichier :

**IMPORTER UN FICHIER DANS LA PKI**

Fichier à importer:  ...

Format du fichier:  P12  DER  PEM

Mot de passe du fichier (si PKCS#12):

Éléments à importer:  Tous  Certificat(s)  Clé(s) privée(s)  CRL  CA

Écraser le contenu existant dans la PKI

- J'observe l'apparition de sns.b.net :

OBJETS / CERTIFICATS ET PKI

Entrer un filtre... Filtre : Tous + Ajouter Révoquer Actions Télécharger Vérifier l'utilisation

sslvpn-full-default-authority

entreprisea

sns.b.net

SSL proxy default authority

DÉTAILS RÉVOCATION (CRL) PROFILS DE CERTIFICATS

Validité

Dernière mise à jour: Oct 13 16:34:30 2025 GMT

Prochaine mise à jour: Nov 12 16:34:30 2025 GMT

POINTS DE DISTRIBUTION

+ Ajouter X Supprimer

URI (adresse)

CERTIFICATS RÉVOCUÉS

- J'ajoute 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

C=FR ST=France L=Saint-Raphael O=entreprisea OU=entreprisea CN=entreprisea

TUNNELS MOBILES - CLÉS PRÉ PARTAGÉES (DPK)

- Je modifie le correspondant IPsec :

Entrez un filtre...

Passerelles distantes (1)

Site\_Fw\_A

### SITE\_FW\_A

**Général**

Commentaire:

Passerelle distante: Fw\_A

Adresse locale: Any

Profil IKE: IKEPHASE1NOMADE

Version IKE: IKEv2

**Identification**

Méthode d'authentification: Certificat

Certificat: C=FR ST=France L=Saint-Raphael O=entreprisea OU=entreprisea

Local ID: Saisir un identifiant (optionnel)

ID du correspondant: Saisir un identifiant (optionnel)

Clé pré-partagée (PSK):

Configuration avancée

➤ Je choisis la politique de chiffrement :

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

IPsec 01 (01) Actions Deactivate policy

SITE À SITE (GATEWAY-GATEWAY) MOBILE - UTILISATEURS NOMADES

ID	Statut	Local	Remote	Profil	Version	Créé le	Créé par
1	on	Network_internals	Site_Fw_A	Lan_in_A	IPSECPhase2Normade	30	Originally created on 2025-10-13 19:13:18 by...
2	off	PrivateVPN	Site_Fw_A	IPsec	StrongSwan	30	Originally created on 2025-10-09 12:24:20 by...
3	off	GRP NFT IN DMZ1	Site_Fw_A	GRP NFT IN DMZ1 R	strongswan	30	Originally created on 2025-10-06 12:21:33 by...

➤ Je mets en place les règles de filtrages après avoir créer l'objet srv\_ftp\_priv\_A :

## CRÉER UN OBJET

**Machine**

Nom DNS (FQDN)

Réseau

Plage d'adresses

Routeur

Groupe

Protocole IP

Nom de l'objet: srv\_ftp\_priv\_A

Adresse IPv4: 172.16.1.12

Adresse MAC: 01:23:45:67:89:ab (Facultatif)

**Résolution**

Aucune (IP statique)  Automatique

Commentaire:

3	Net-SSLVPN_UDP	passer	Internet	https	Crée le 2025-10-09 17:48:27, par admin (192.168.2.2)
4	Network_in	passer	srv_ftp_priv_A	ftp	Crée le 2025-10-13 19:23:34, par admin (192.168.2.2)
5	Network_in	passer	Any	icmp (requête Ech...	Crée le 2025-10-13 19:24:03, par admin (192.168.2.2)

➤ Puis je ping pour tester :

```

user@client-training: ~ 80x24
user@client-training:~$ ping 172.16.1.12
PING 172.16.1.12 (172.16.1.12) 56(84) bytes of data.
64 bytes from 172.16.1.12: icmp_seq=1 ttl=64 time=4.77 ms
64 bytes from 172.16.1.12: icmp_seq=2 ttl=64 time=5.23 ms
^C
--- 172.16.1.12 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3ms
rtt min/avg/max/mdev = 4.773/5.001/5.229/0.228 ms
user@client-training:~$

```

➤ Et enfin je regarde les tunnels dans la supervision ainsi que les logs vpn :

### MONITOR / TUNNELS VPN IPSEC

Actualiser Configurer le service VPN IPsec

**POLITIQUES**

Type	État	Extrémité de trafic loc...	Passerelle locale	Local ID	Passerelle distante	ID du correspon...	Extrémité de trafic dis...
Type : Tunnels site à site (4)							
🔌	OK	Network_dmz1	Firewall_out	C=FR, ST=Franc...	Fw_A	%any	Lan_in_A
🔌	OK	Network_in	Firewall_out	C=FR, ST=Franc...	Fw_A	%any	Lan_in_A
🔌	OK	Net-SSLVPN_TCP	Firewall_out	C=FR, ST=Franc...	Fw_A	%any	Lan_in_A
🔌	OK	Net-SSLVPN_UDP	Firewall_out	C=FR, ST=Franc...	Fw_A	%any	Lan_in_A
Type : Politiques d'exception (bypass) (1)							
	Bypass	rfc5735_loopback	localhost		localhost		any

Association de sécurité (SA) IKE

Aucune association de sécurité n'a été trouvée pour cette SPD (Security Policy Database)

### LOG / VPN

Dernière heure Actualiser Rechercher... Recherche avancée Actions

RECHERCHE DU - 13/10/2025 18:30:46 - AU - 13/10/2025 19:30:46

Enregistré à	Message	Utilisateur	Nom de la source	Réseau local	Nom de destination	Réseau distant	DÉTAILS DE LA LIGNE DE LOG
13/10/2025 19:21:40	IPSEC SA established		Firewall_out	192.168.2.0/24	Fw_A	192.168.1.0/24	Configuration
13/10/2025 19:21:40	Narrowing from 172.30.2.1/32 172.31.2.1/32 172.16.2.0/24 192.168.2.0/24 172.31.2.0/24 172.30.2...		Firewall_out	192.168.2.0/24	Fw_A	192.168.1.0/24	Nom de la règle 199de220fe9_7
13/10/2025 19:21:27	IPSEC SA established		Firewall_out	192.168.2.0/24	Fw_A	192.168.1.0/24	Type de règle gateway
13/10/2025 19:21:27	Narrowing from 172.30.2.1/32 172.31.2.1/32 172.16.2.0/24 192.168.2.0/24 172.31.2.0/24 172.30.2...		Firewall_out	192.168.2.0/24	Fw_A	192.168.1.0/24	Dates
13/10/2025 19:21:26	Charon configuration reloaded						Enregistré à 13/10/2025 19:21:40
13/10/2025 19:21:26	IPSEC SA deleted		Firewall_out	192.168.2.0/24	Fw_A	192.168.1.0/24	Date et heure 13/10/2025 19:21:40