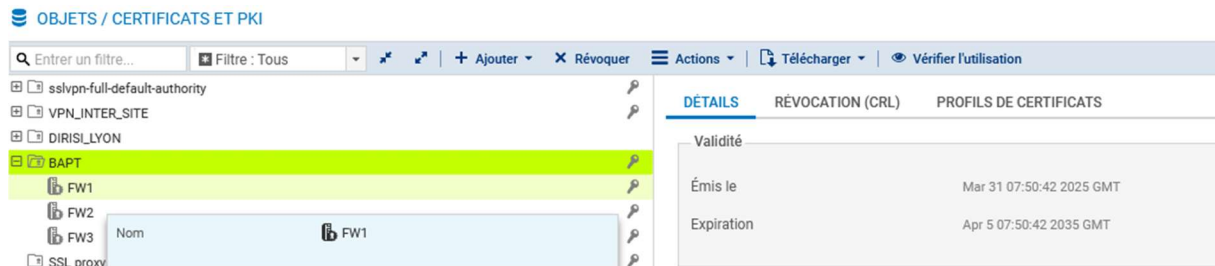
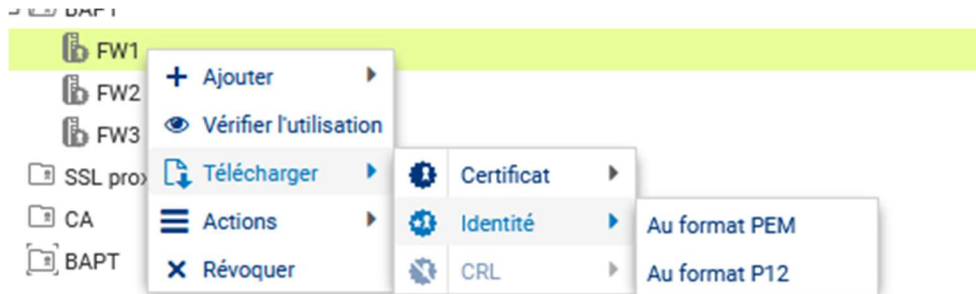


VPN IPsec Stormshield

J'ai commencé par créer une autorité de certificat ainsi que trois identités serveur dans l'autorité de certificats. J'ai réalisé tout ça dans mon firewall 3 car le firewall3 est le centre de la topologie du vpn car il y a deux tunnels, entre le fw1 et fw3 ; f2 et fw3.



J'ai donc importé les identités serveurs en téléchargeant l'identité au format P12 qui permet d'importer aussi la clé privée.



J'ai ensuite ajouté tout ça dans le SMC (Stormshield Management Center) qui va gérer le vpn entre les trois firewalls.

Nom	Statut du certificat	Date de début	Date de fin	Firewall	Dossier	Topologies
BAPT	Valide	31/03/2025	05/04/2035			VPN-BAPT
FW1	Valide	06/04/2025	07/04/2026	LYO_FWL_1	My SMC LA	VPN-BAPT
FW2	Valide	06/04/2025	07/04/2026	LYO_FWL_2	My SMC LA	VPN-BAPT
FW3	Valide	06/04/2025	07/04/2026	LYO_FWL_3	My SMC LA	VPN-BAPT

J'ai ensuite créer la topologie vpn .

TOPOLOGIES VPN / TOPOLOGIE VPN-BAPT

Étape 3/4 : Choix des correspondants



Veillez choisir ici les firewalls SNS et les machines qui participent à la topologie VPN.

Centre de la topologie: LYO_FWL_3 Ne pas initier les tunnels (Responder-only) ☐

Rechercher...	État	Nom	Action	Certificat pour l'...	Version	Réseau géré par...	Lieu
	☒	LYO_FWL_1		C=FR,ST=zrgh...	4.8.6	☒	
	☒	LYO_FWL_2		C=FR,ST=zrgh...	4.8.6	☒	
	☒	LYO_FWL_3		C=FR,ST=zrgh...	4.8.6	☒	

Après dans chaque firewall il a fallu configurer les correspondant :

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

Local

Entrer un filtre... + Ajouter Actions

Passerelles distantes (2)

Site_3

vpn-bapt3

VPN-BAPT3

Général

Commentaire

Passerelle distante: PUB_FWL_3

Adresse locale: Any

Profil IKE: StrongEncryption

Version IKE: IKEv2

Identification

Méthode d'authentification: Certificat

Certificat: C=FR ST=zrgh L=zrtgh O=rtg OU=z'gtr CN=BAPT.C=FR ST=zrgh L=zrtgh O=rtg OU=z'

Local ID: Saisir un identifiant (optionnel)

ID du correspondant: CN=FW3

Clé pré-partagée post-quantique (PPK)

L'identification :

AUTORITES DE CERTIFICATION ACCEPTEES

+ Ajouter X Supprimer

CA

C=FR ST=RHONE L=LYON O=DIRISI OU=CMORD CN=VPN_INTER_SITE

C=FR ST=Lyon L=Lyon O=test OU=test CN=CA-VPN-Stormshield

CA

C=FR ST=zrgh L=zrtgh O=rtg OU=z'gtr CN=BAPT

La dernière étape la plus importante est d'importer la CRL du firewall 3 dans les deux autres firewalls car la CRL (Certificate Revocation List) est un mécanisme de sécurité utilisé pour vérifier qu'un certificat n'a pas été annulé.

Sans ça le vpn ne peut pas fonctionner.



Et voilà le résultat :

✓	* VPN-BAPT	Par route	VTI_on_LYO_FWL_3_with_LYO_FWL_1_in_
✓	* VPN-BAPT	Par route	VTI_on_LYO_FWL_3_with_LYO_FWL_2_in_