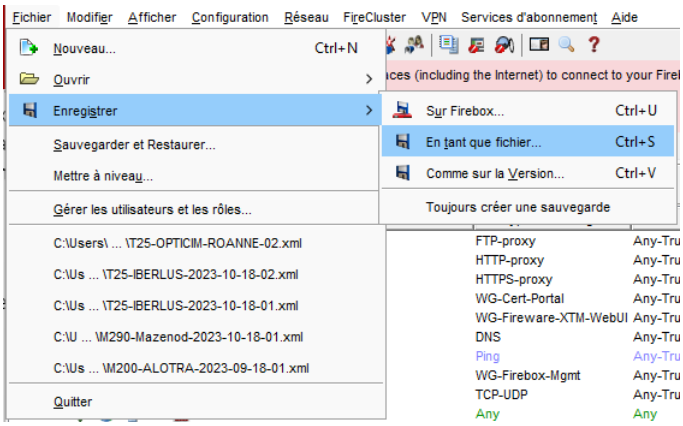
REMPLACEMENT Boitier WatchGuard

Procédure WG – [AP 2023/10]

ETAPE 1 – Récupération de la config du boitier en place

Se connecter sur le Boitier en fonctionnement. Grâce à Policy Manager, récupérer la config sur son PC.



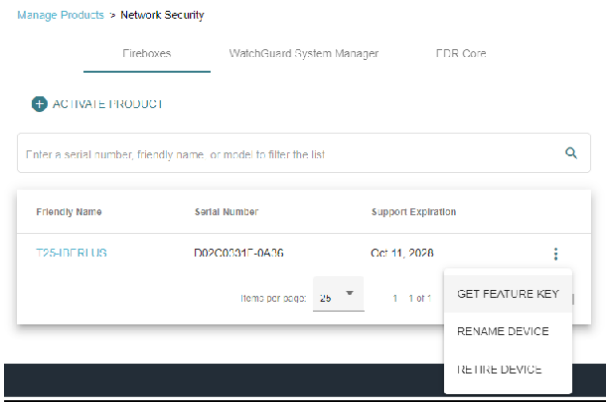
ETAPE 2 – Ajouter le nouveau boitier sur l'interface client WatchGuard

Se connecter au portail www.watchguard.com avec les identifiants du client (voir fiche info).

Si des licences supplémentaires sont nécessaires (par ex : APT-blocker), les rajouter de la même manière.

Nb : Si une demande de changement de mot de passe apparait, la faire et **bien renseigner le nouveau mot de passe dans la fiche info**

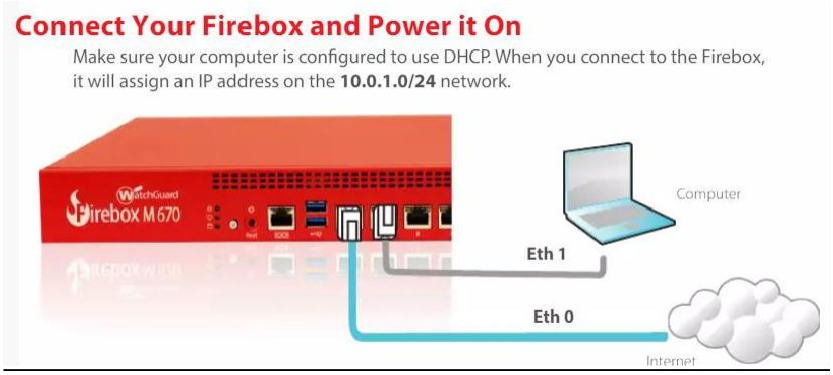
Une fois le boitier ajouté correctement avec toutes ses licences, télécharger les clefs (Feature Key) dans :
My WatchGuard > **Manage Products** > **Network Security**



Enregistrer dans un fichier texte, cela nous servira plus tard.

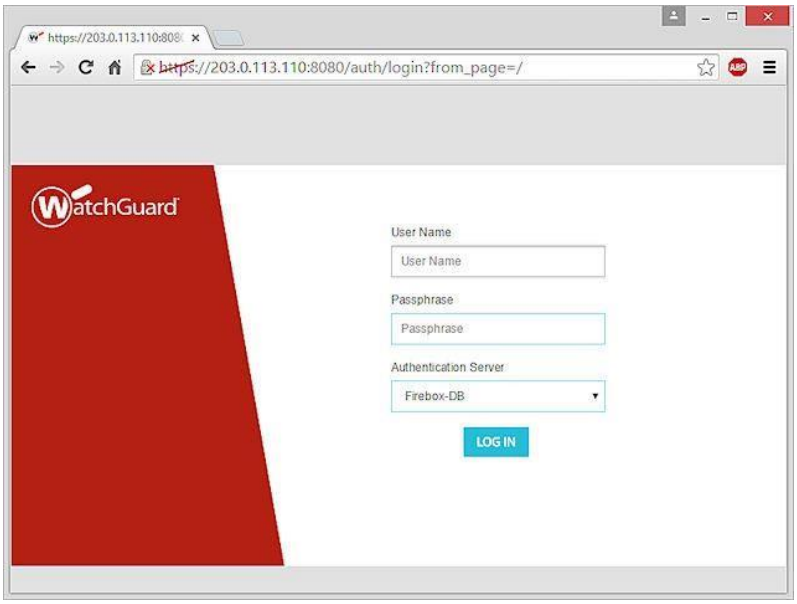
ETAPE 3 – Initialiser le nouveau boitier

Démarrer puis connecter le boitier de cette manière ;
#ETH0 = Réseau avec accès internet
#ETH1 = Un PC en DHCP

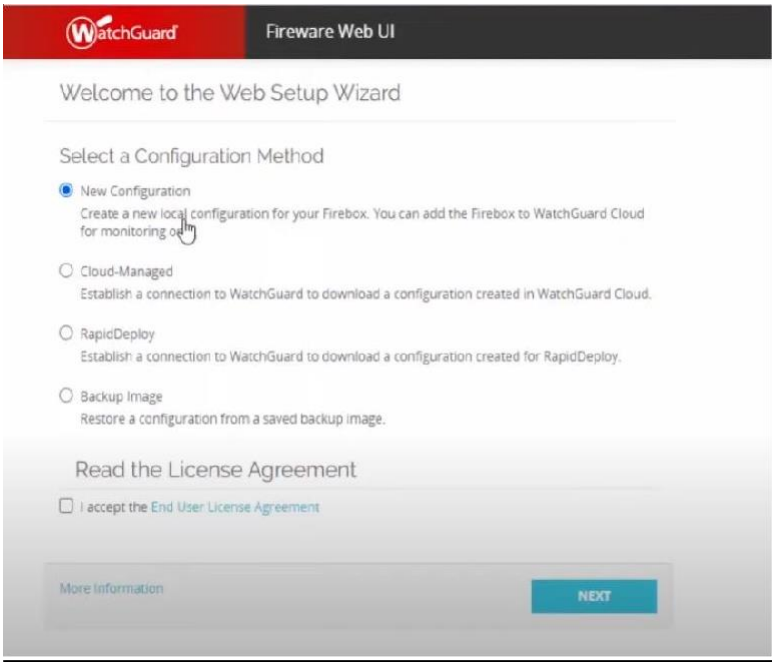


Se connecter ensuite au Web UI sur https://10.0.1.1:8080

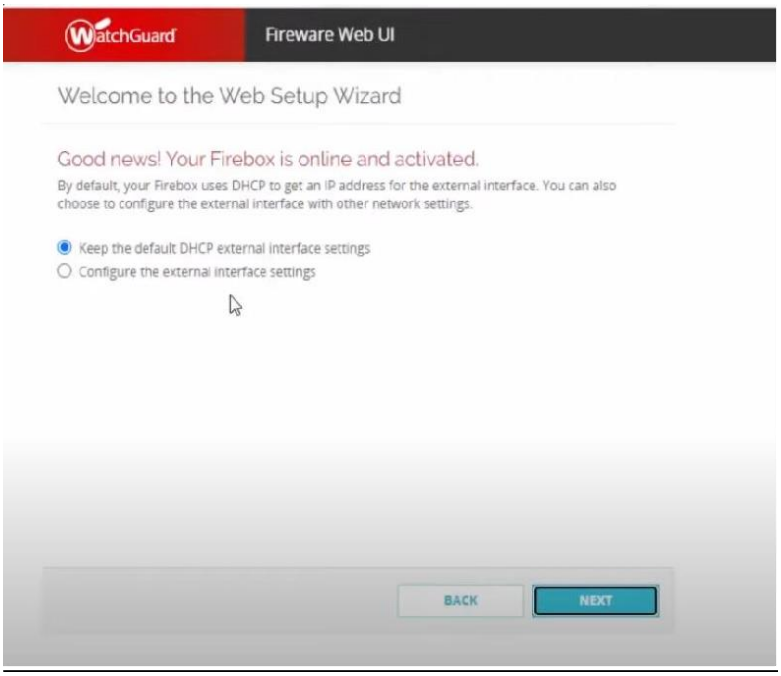
Login : *****
Password : *****



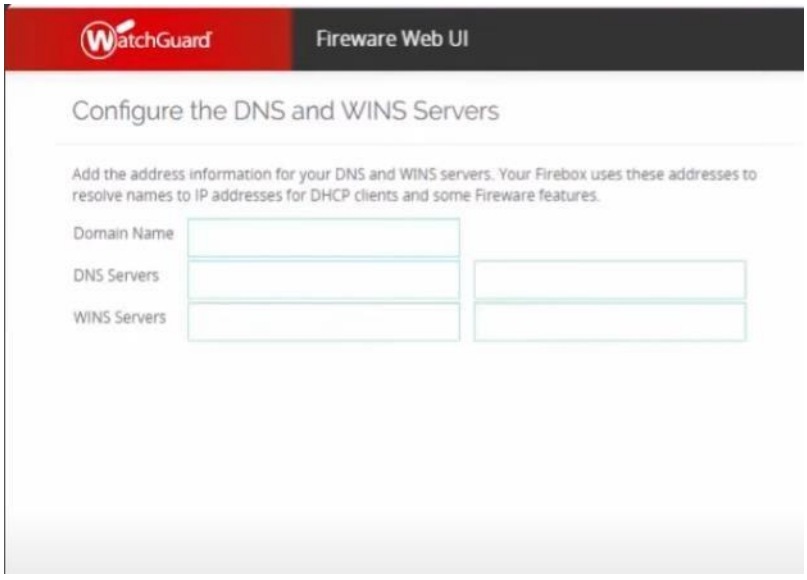
Choisir **« New Configuration »**.



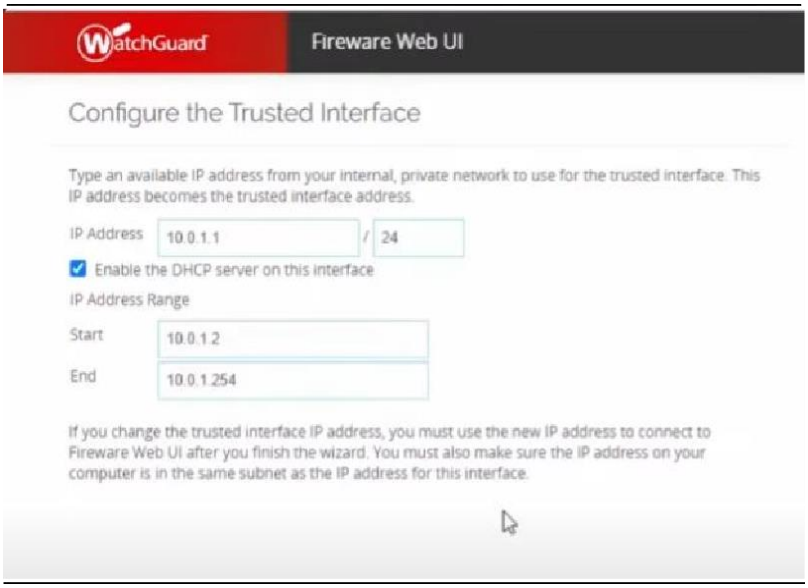
Laisser en DHCP l'interface externe (**#ETH0**)



Renseigner les DNS **8.8.8.8** et **1.1.1.1**

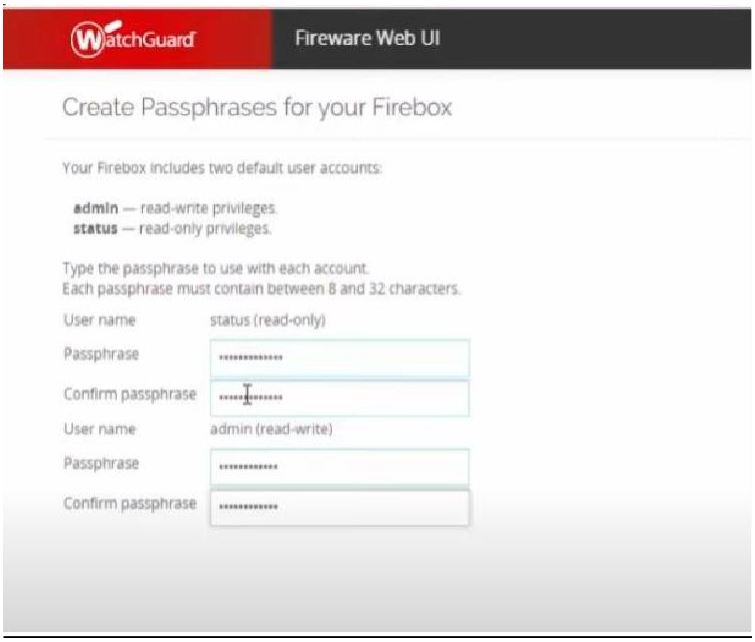


Laisser l'interface #ETH1 par défaut :
10.0.1.1/24

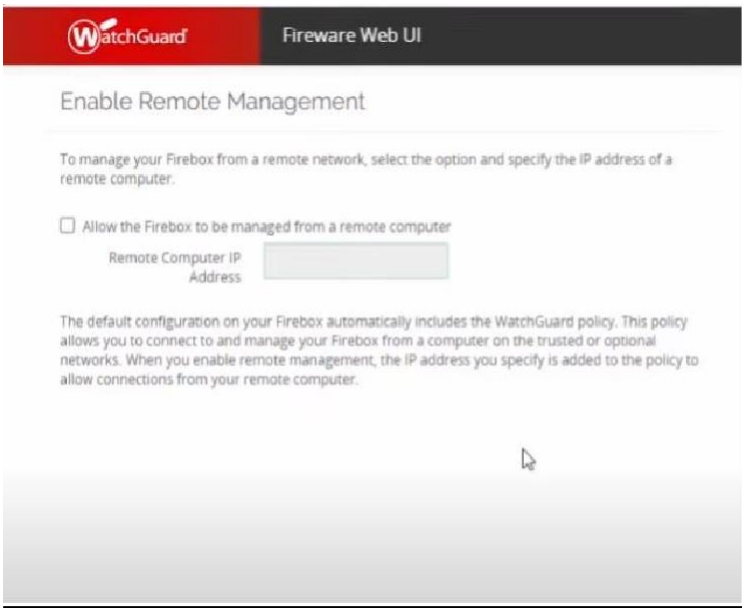


Configurer les identifiants ***status*** et ***admin*** **avec les mêmes que ceux de l'ancien boitier.**

Récupérer les infos dans la fiche client.



Ne pas configurer cette partie.

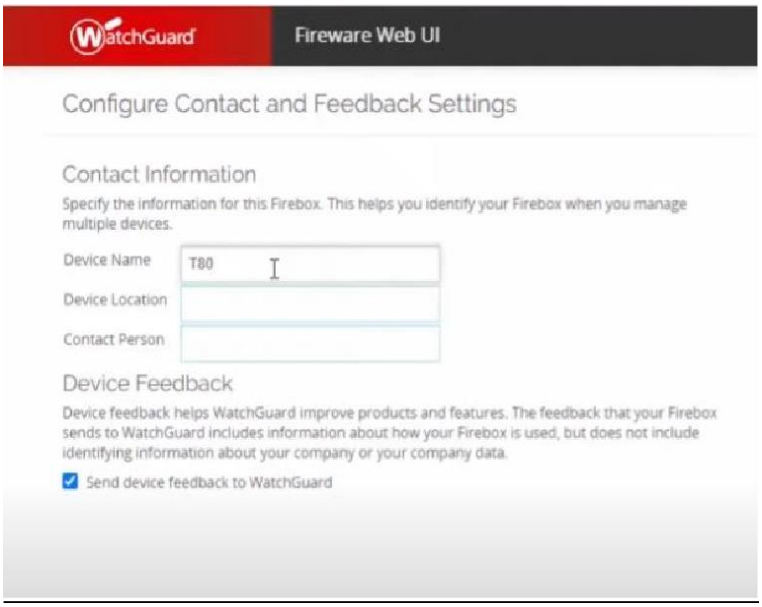


Device Name : BOITIER-CLIENT
(Exemple : « ***T80-NOM*** »)

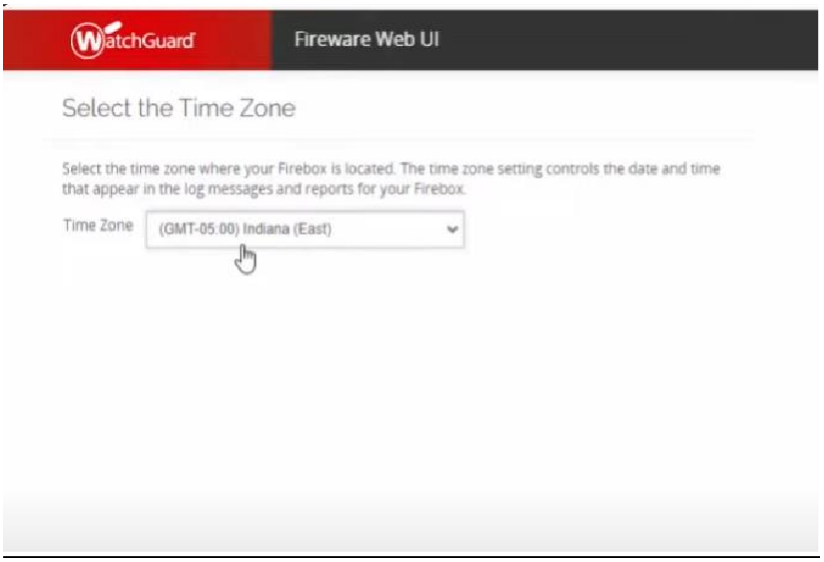
Device Location : CODE-POSTAL VILLE
(Exemple : « ***13005 Marseille*** »)

Contact Person : « *********** »

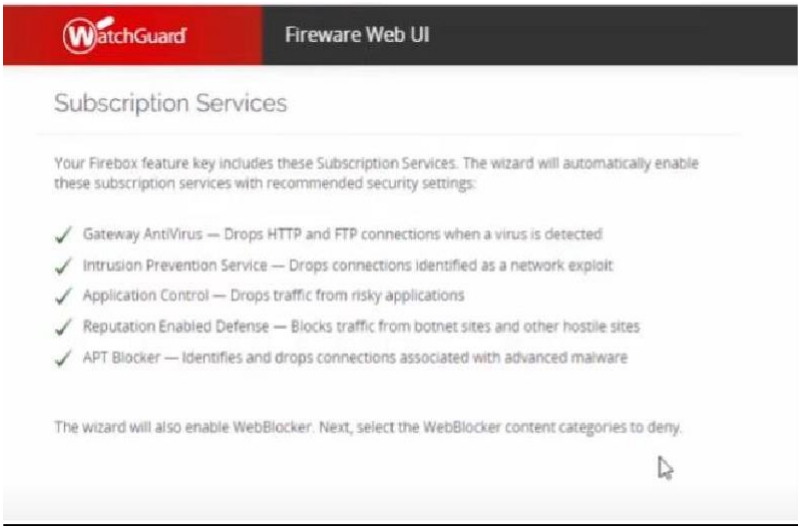
Device Feedback : Décocher.



Configurer la bonne time zone.

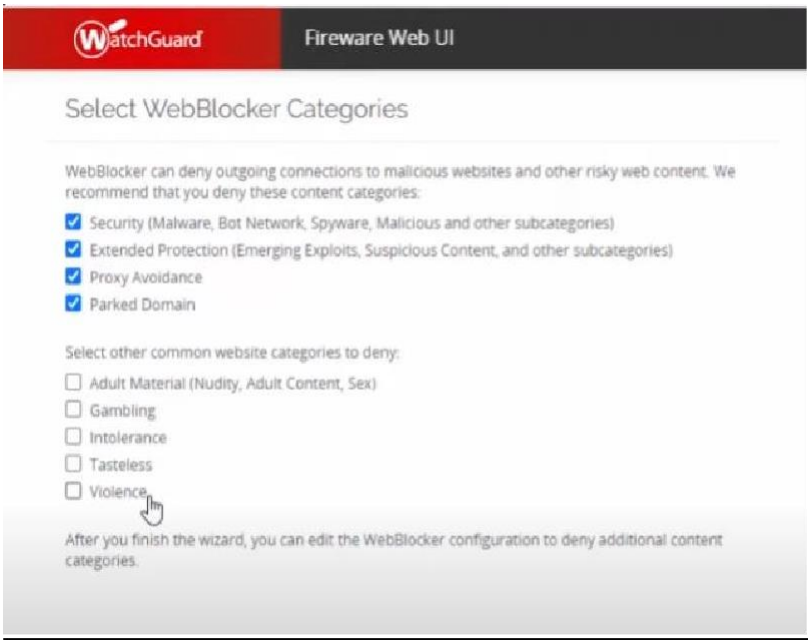


Faire **Next**



Faire **Next** également

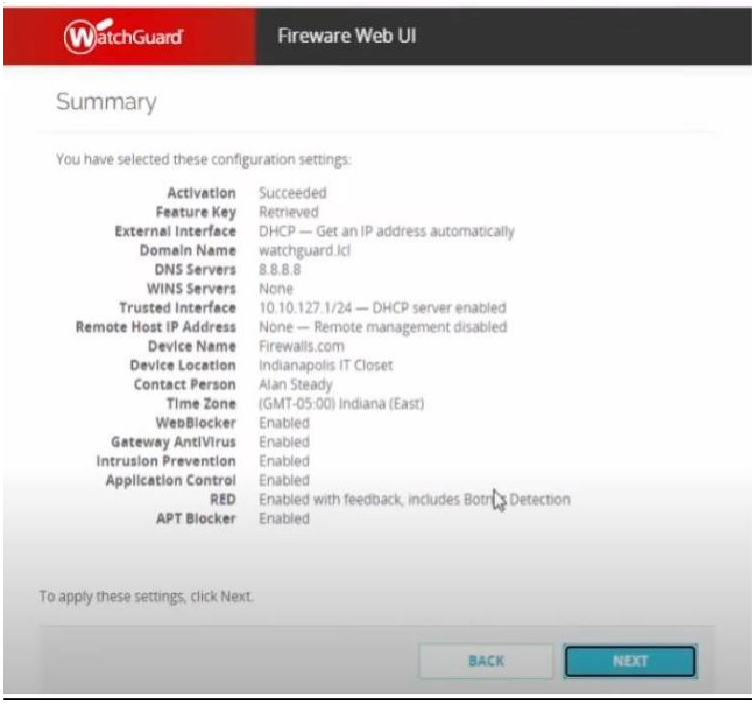
(Tout paramétrage est inutile car on va tout « écraser » en réinjectant la config)



Le dernier écran est simplement un récap de tout ce qu'on a configurer.

Vérifier les infos et faire ***Next.***

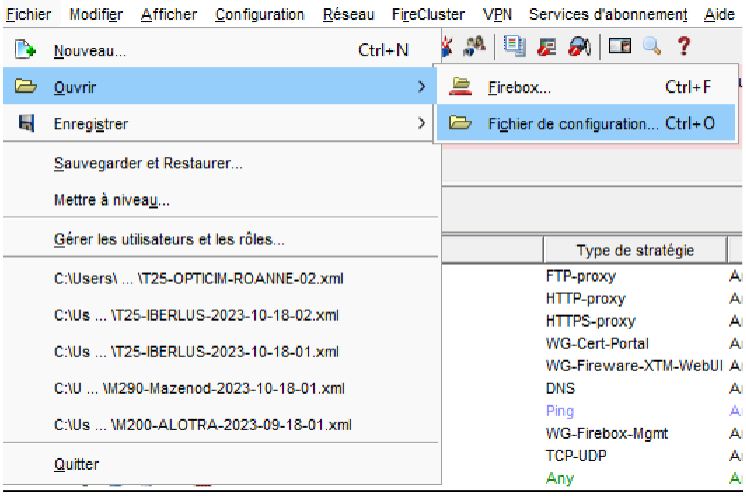
Le boitier est maintenant initialisé.



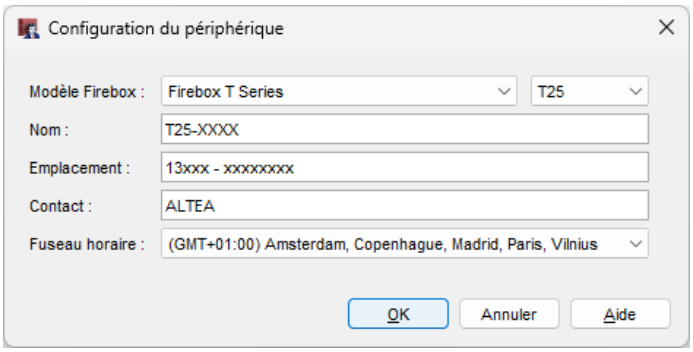
ETAPE 4 – Injecter la configuration

Sur WatchGuard System Manager (à télécharger sur www.watchguard.com), ouvrir le Policy Manager.

Ouvrir le fichier de config préalablement récupéré à l'étape1



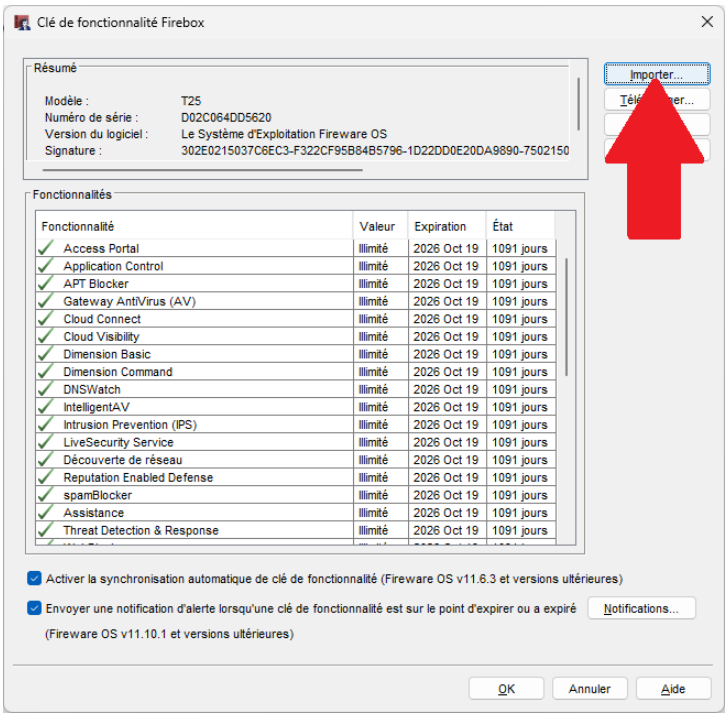
Modifier les paramètres de périphérique avec les bonnes infos du nouveau boitier :
Configuration > Système



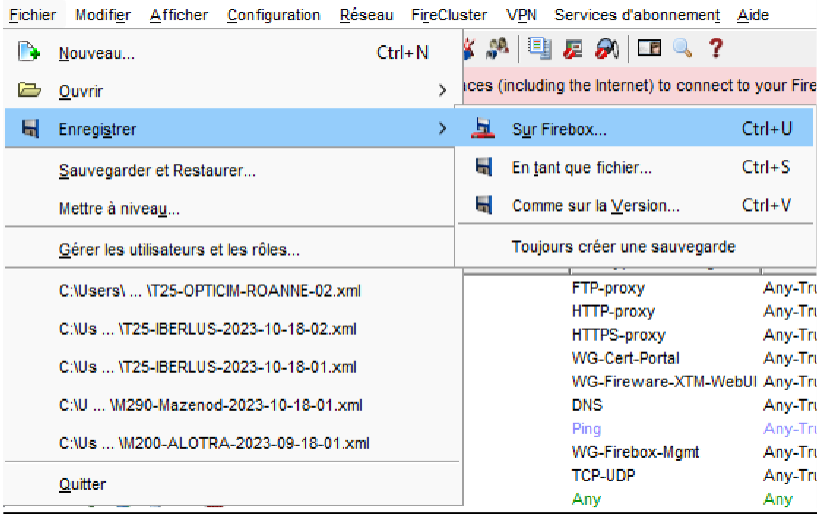
Configuration > Clef de fonctionnalités

Vérifier que la licence soit opérationnelle.

Si ce n'est pas le cas, importer le fichier de licences (récupéré à l'étape 2) dans le boitier.



Enregistrer ensuite la config sur le boitier
Fichier > Enregistrer > Sur Firebox



ETAPE 5 – Paramétrages spécifiques et vérifications

Faire les paramétrages spécifiques au client et faire des tests pour valider le fonctionnement.

Par exemple (liste non exhaustive, à adapter à la situation) :

- Si dans la box du client il y a une réservation DHCP avec l'adresse MAC du WatchGuard ➔ Renseigner l'adresse MAC du nouveau WatchGuard (eth0) et vérifier qu'il prenne la bonne IP.
- Si le client a un VPN externe SSL, vérifier en partage de connexion que cela fonctionne.
- Si le client a un VPN IPsec, vérifier que le lien soit bien monté.
- Vérifier que les utilisateurs aient bien accès à internet et à leur serveur.
- Vérifier que le serveur ait bien accès internet/anydesk.
- Se connecter sur le nouveau boitier et vérifier que tout soit ok (pas d'erreur de licences par exemple)
- Si le boitier était accessible à distance, vérifier que cela fonctionne.
- Etc…

Contexte

J’ai utilisé cette procédure pour faire le remplacement du WatchGuard qui est arrivé à expiration dans une entreprise, le WatchGuard sert de pare-feu avec un filtrage qui permet de bloquer une partie des malwares, ransomwares, fishing par email et il permet un control sur la navigation des utilisateurs de l’entreprise. Il peut etre configurer pour ouvrir un tunnel sécurisé entre le réseau de l’entreprise et l’extérieur : le VPN.