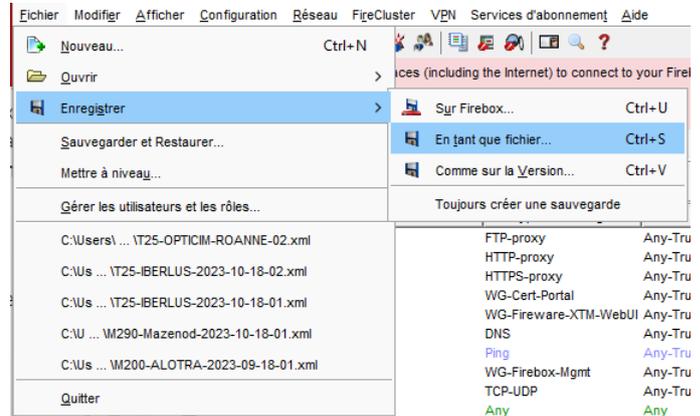


REMPACEMENT Boitier WatchGuard

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.

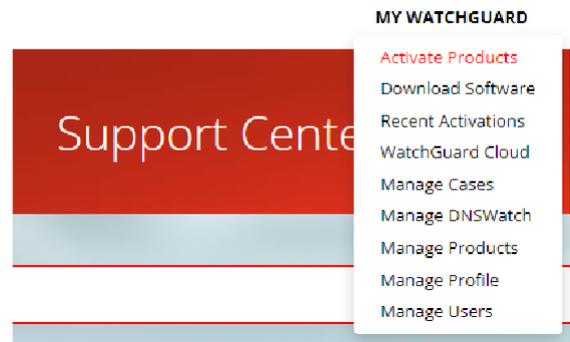


ETAPE 2 – Ajouter le nouveau boitier sur l'interface client WatchGuard

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.

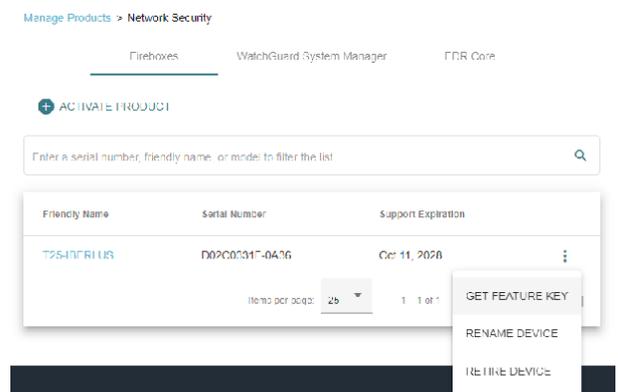
Nb : Si une demande de changement de mot de passe apparait, la faire et **bien renseigner le nouveau mot de passe dans la fiche info**



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 boîtier

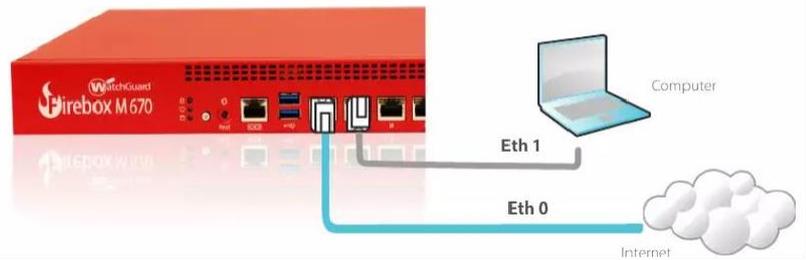
Démarrer puis connecter le boîtier de cette manière ;

#ETH0 = Réseau avec accès internet

#ETH1 = Un PC en DHCP

Connect Your Firebox and Power it On

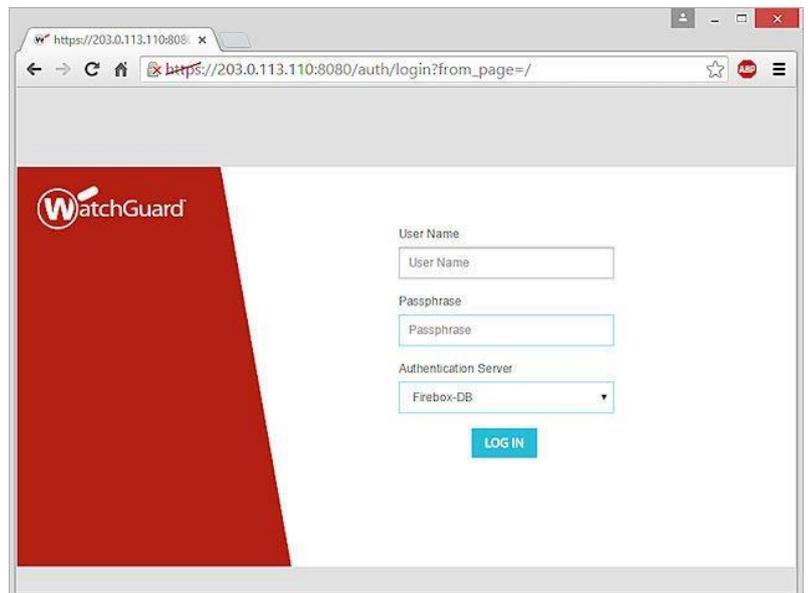
Make sure your computer is configured to use DHCP. When you connect to the Firebox, it will assign an IP address on the 10.0.1.0/24 network.



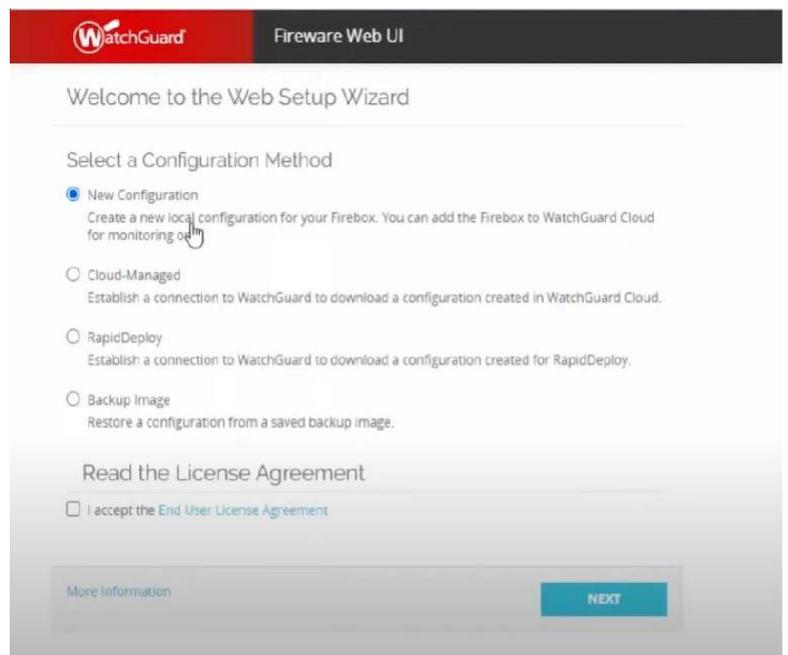
Se connecter ensuite au Web UI sur <https://10.0.1.1:8080>

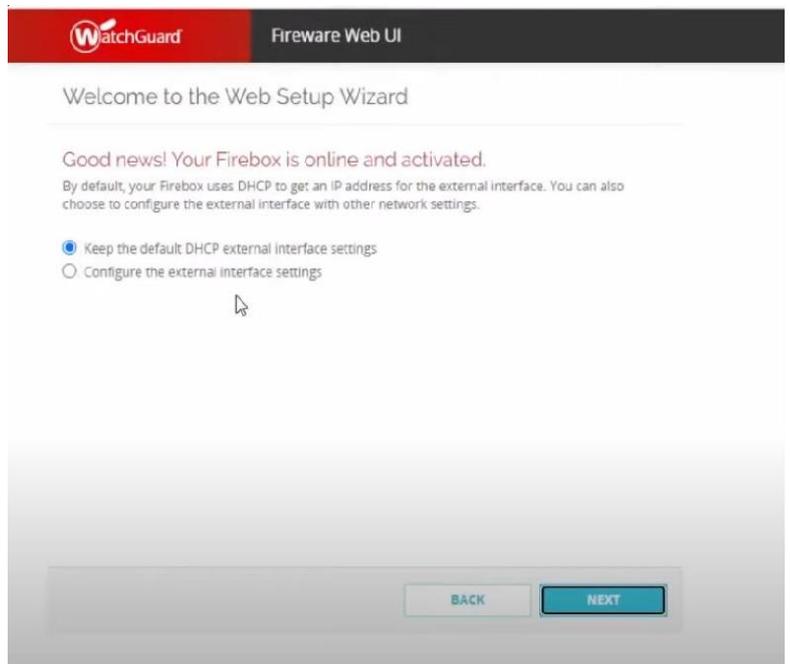
Login : *****

Password : *****

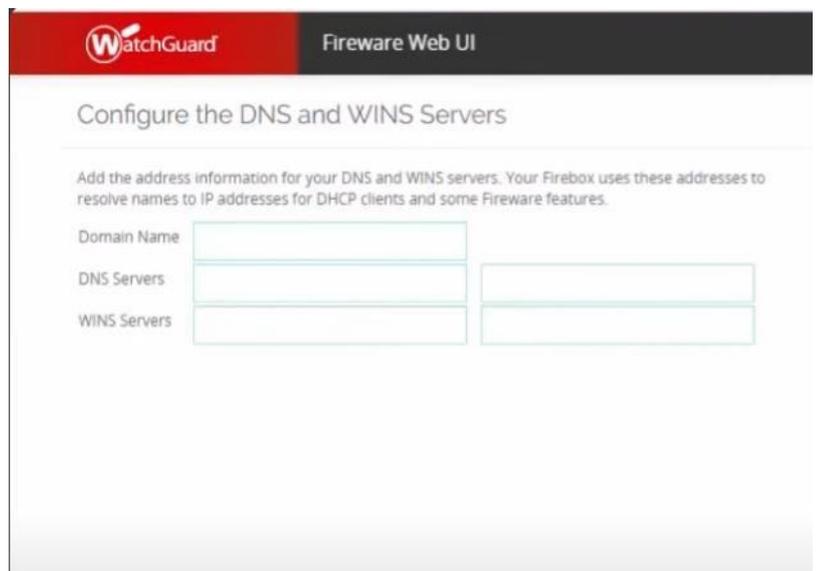


Choisir « New Configuration ».





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 boîtier.

Récupérer les infos dans la fiche client.

The screenshot shows the 'Create Passphrases for your Firebox' page in the WatchGuard Fireware Web UI. It lists two default user accounts: 'admin' (read-write privileges) and 'status' (read-only privileges). Below, there are two sets of input fields for creating passphrases. The first set is for the 'status (read-only)' user, and the second is for the 'admin (read-write)' user. Each set includes fields for 'User name', 'Passphrase', and 'Confirm passphrase'. The passphrases are masked with dots.

Ne pas configurer cette partie.

The screenshot shows the 'Enable Remote Management' page in the WatchGuard Fireware Web UI. It contains a checkbox labeled 'Allow the Firebox to be managed from a remote computer'. Below the checkbox is a text input field for 'Remote Computer IP Address'. A mouse cursor is visible over the page. Below the form, there is a paragraph of text explaining the default configuration and the effect of enabling remote management.

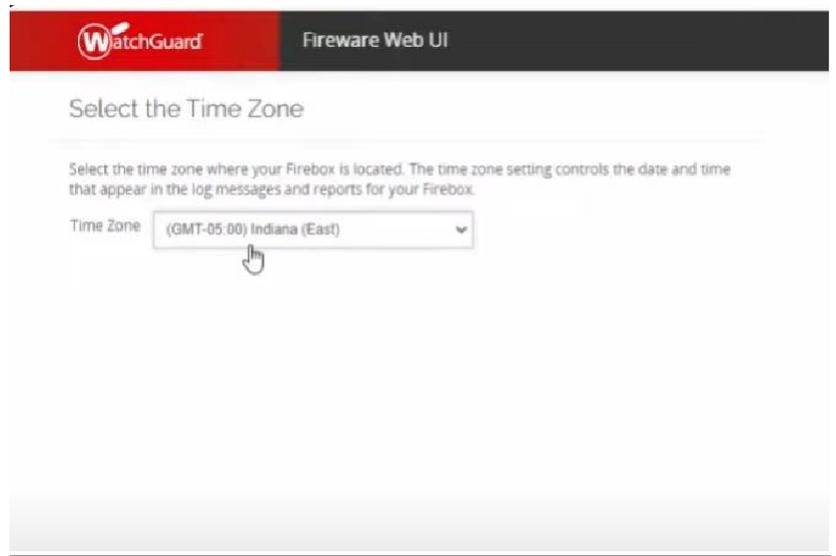
Device Name : BOITIER-CLIENT
(Exemple : « **T80-NOM** »)

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

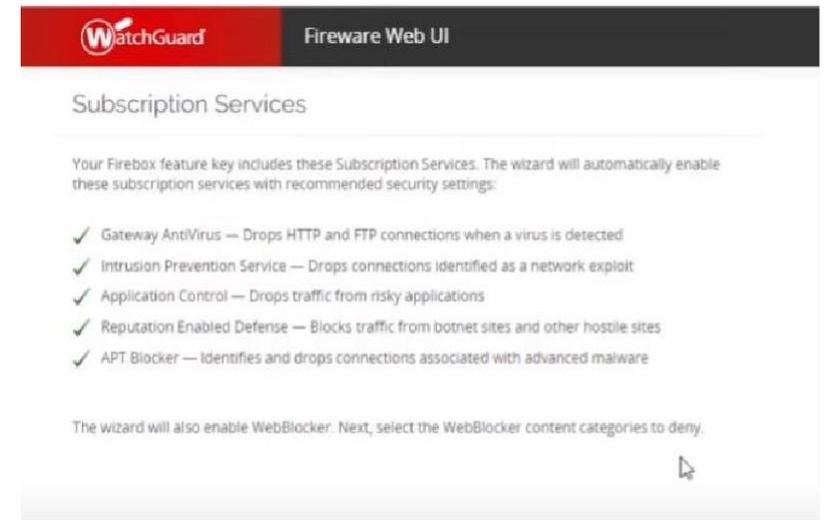
Contact Person : « ***** »

Device Feedback : Décocher.

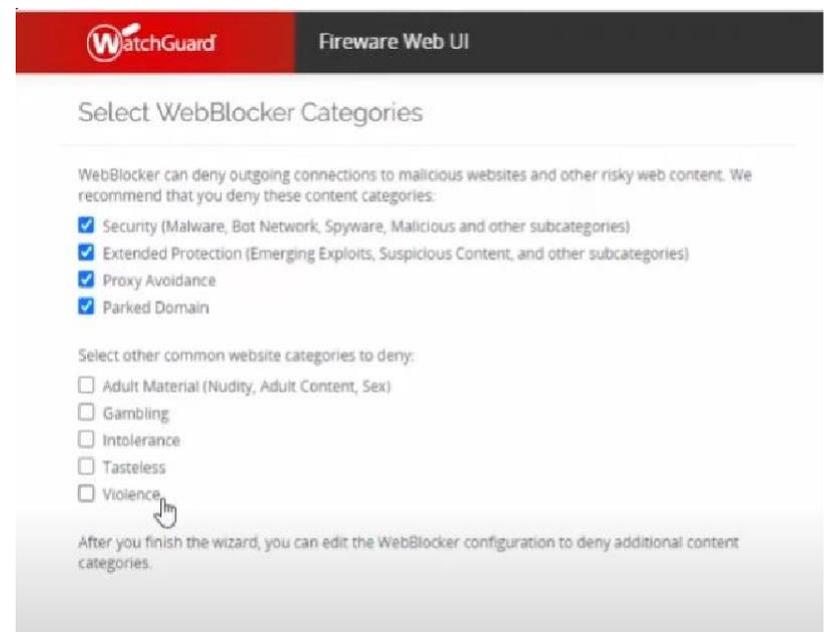
The screenshot shows the 'Configure Contact and Feedback Settings' page in the WatchGuard Fireware Web UI. It is divided into two sections: 'Contact Information' and 'Device Feedback'. The 'Contact Information' section has three input fields: 'Device Name' (containing 'T80'), 'Device Location', and 'Contact Person'. The 'Device Feedback' section has a checkbox labeled 'Send device feedback to WatchGuard', which is currently checked.



Configurer la bonne time zone.

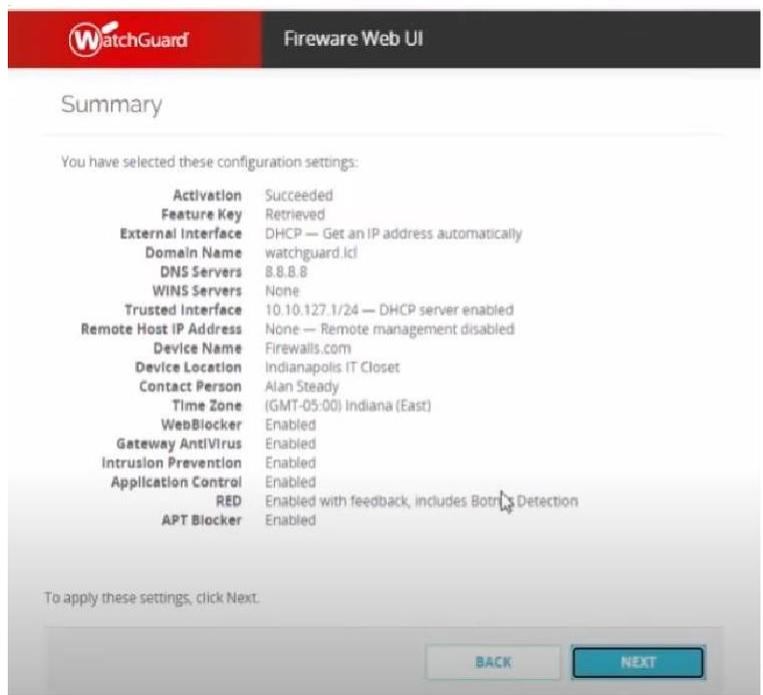


Faire **Next**



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 configuré.

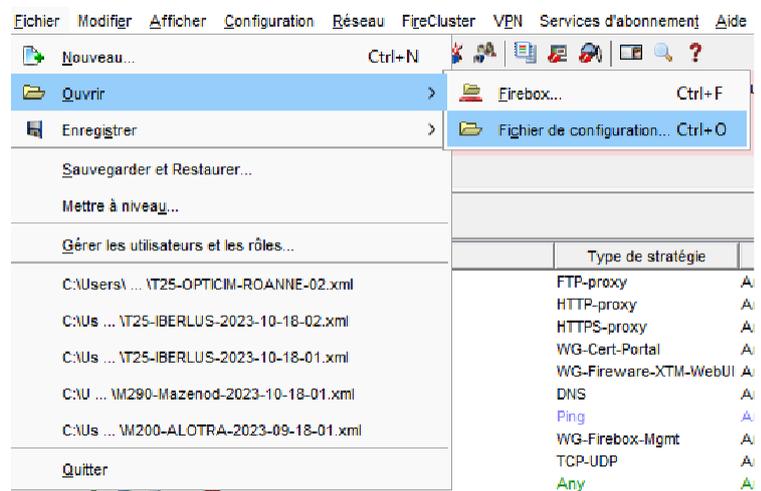
Vérifier les infos et faire **Next**.

Le boîtier est maintenant initialisé.

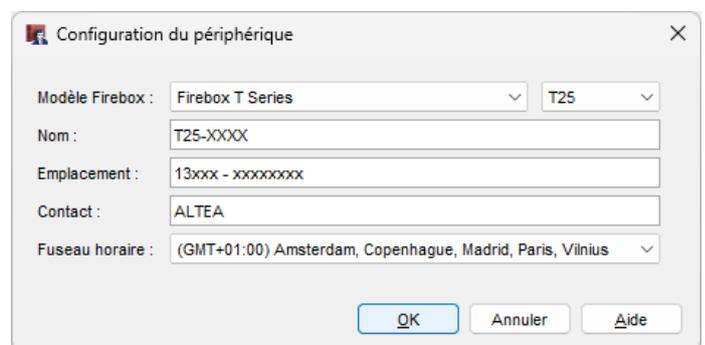
ETAPE 4 – Injecter la configuration

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

Ouvrir le fichier de config préalablement récupéré à l'étape 1



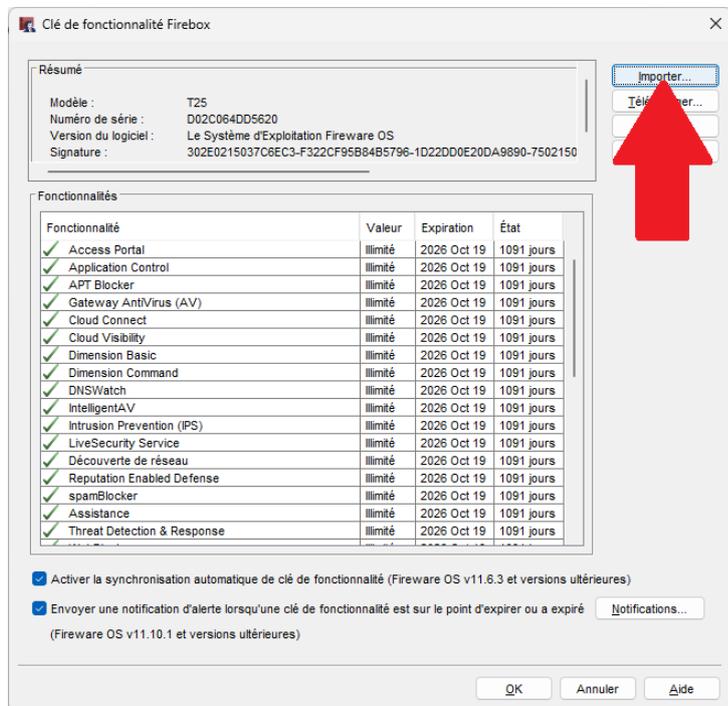
Modifier les paramètres de périphérique avec les bonnes infos du nouveau boîtier : **Configuration > Système**



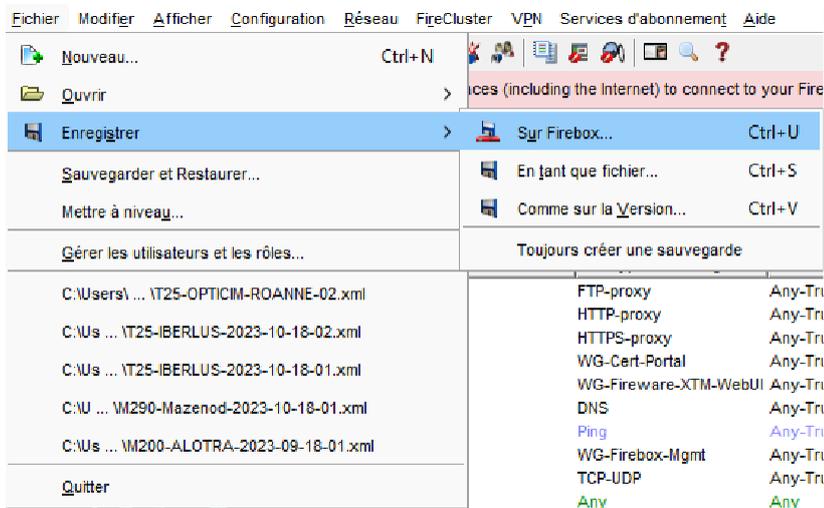
Configuration > Clef de fonctionnalités

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 boîtier.



Enregistrer ensuite la config sur le boîtier
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 boîtier et vérifier que tout soit ok (pas d'erreur de licences par exemple)
- Si le boîtier 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, phishing 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.
