Rapport SAE 401 : Sécurisation d’un SI

Participant : AZIZ Souhayl

Tâche 4 : Authentification transparente par certificat SSL (Secure Sockets Layer)

Pour rappel, voici notre plan IP :

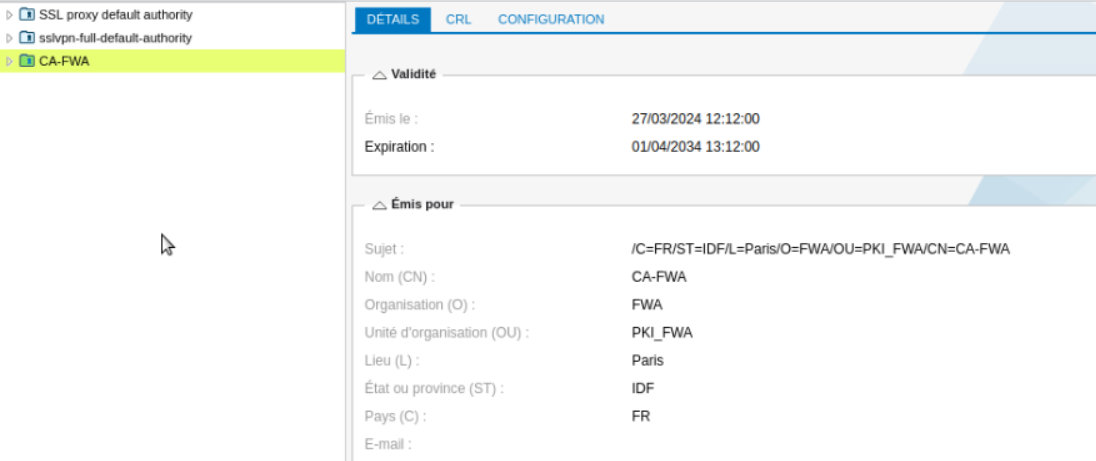
Une image contenant texte, diagramme, capture d’écran, ligne

Description générée automatiquement

Une image contenant texte, capture d’écran, Police, ligne

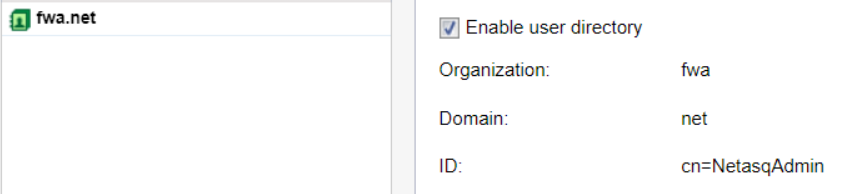
Description générée automatiquement

Pour cette tâche, nous avons dans un premier temp créé une autorité racine et l’avons défini par défaut :

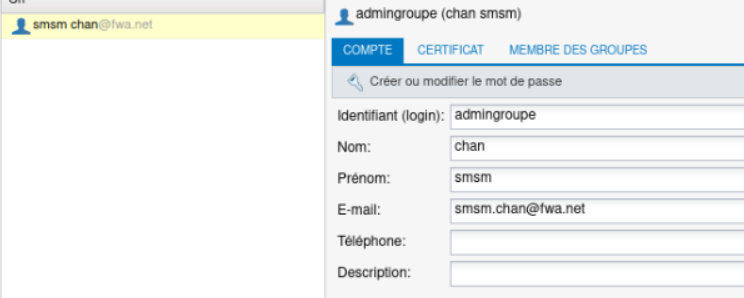


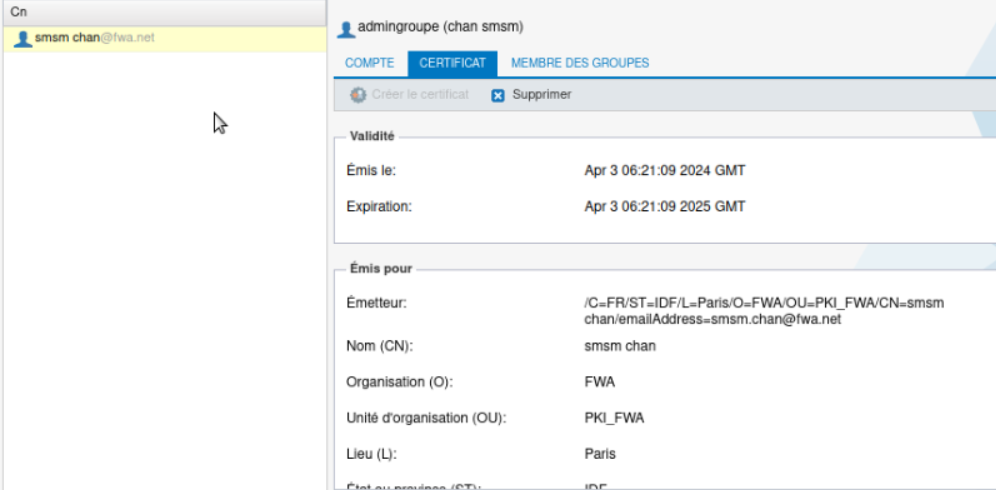
Activation de l’authentification :

Pour pouvoir activer l’authentification il faut créer un annuaire LDAP pour y ajouter des utilisateurs.



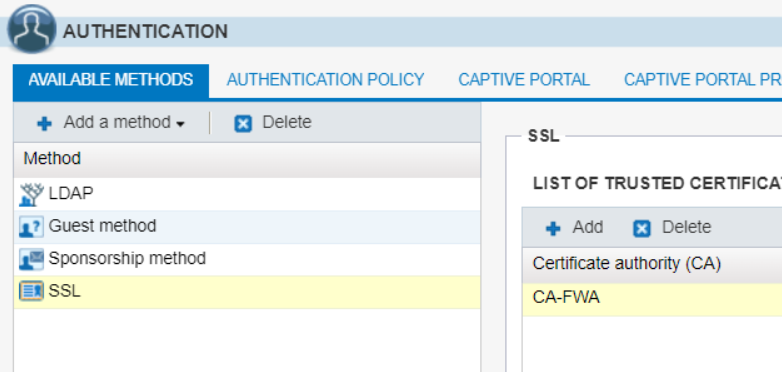
Ensuite, on a créé un utilisateur avec son certificat pour qu’on puisse s’authentifier avec :



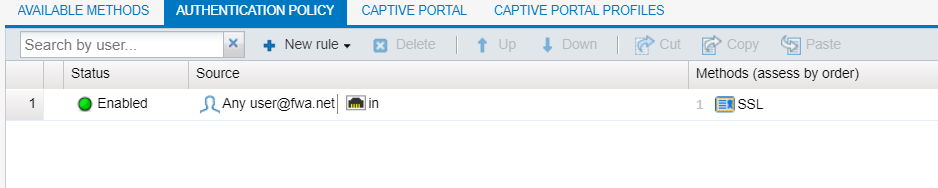


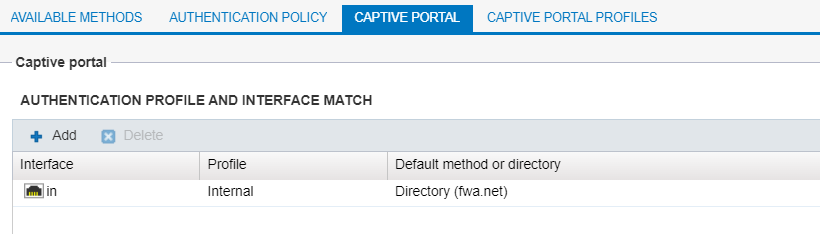
Mise en place et test :

Pour finir la validation, on ajoute une méthode d’authentification SSL et on définit son certificat d’autorité

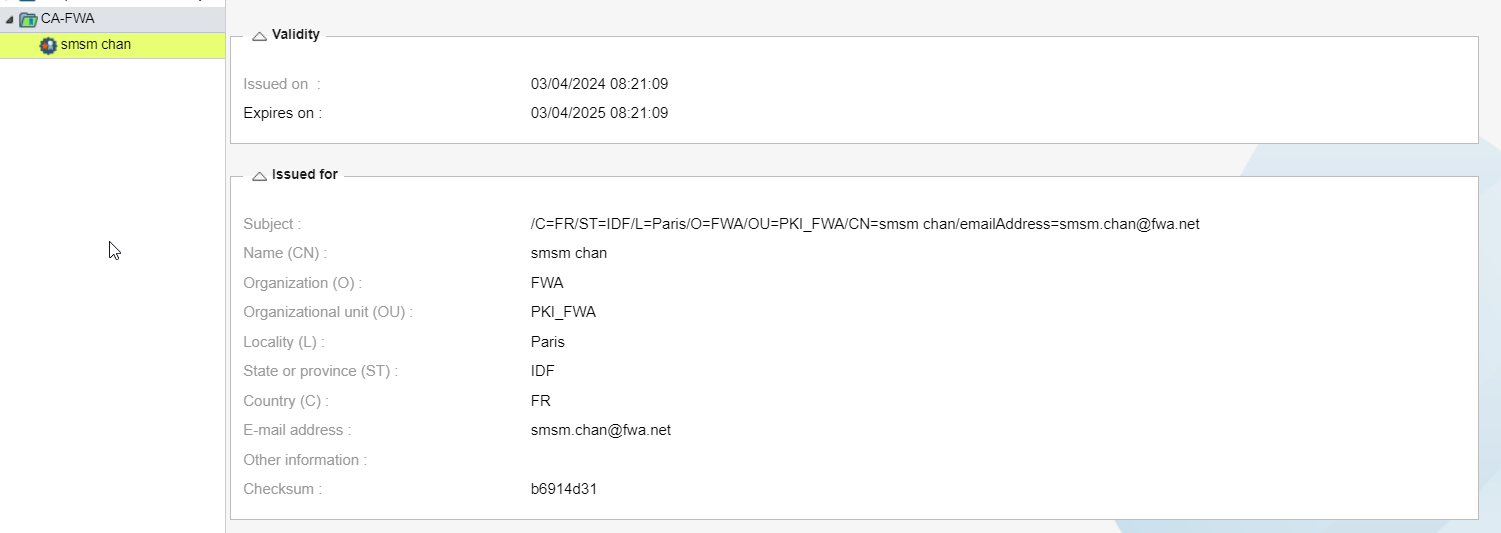


On définit ensuite une règle d’authentification par certificat SSL





On télécharge ensuite au format P12 le certificat de l’utilisateur depuis le Certificat d’Autorité

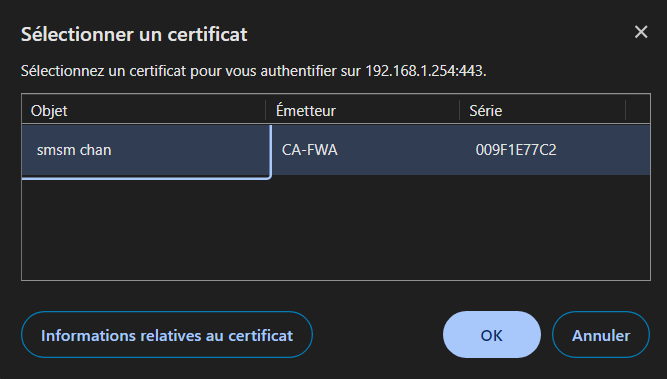


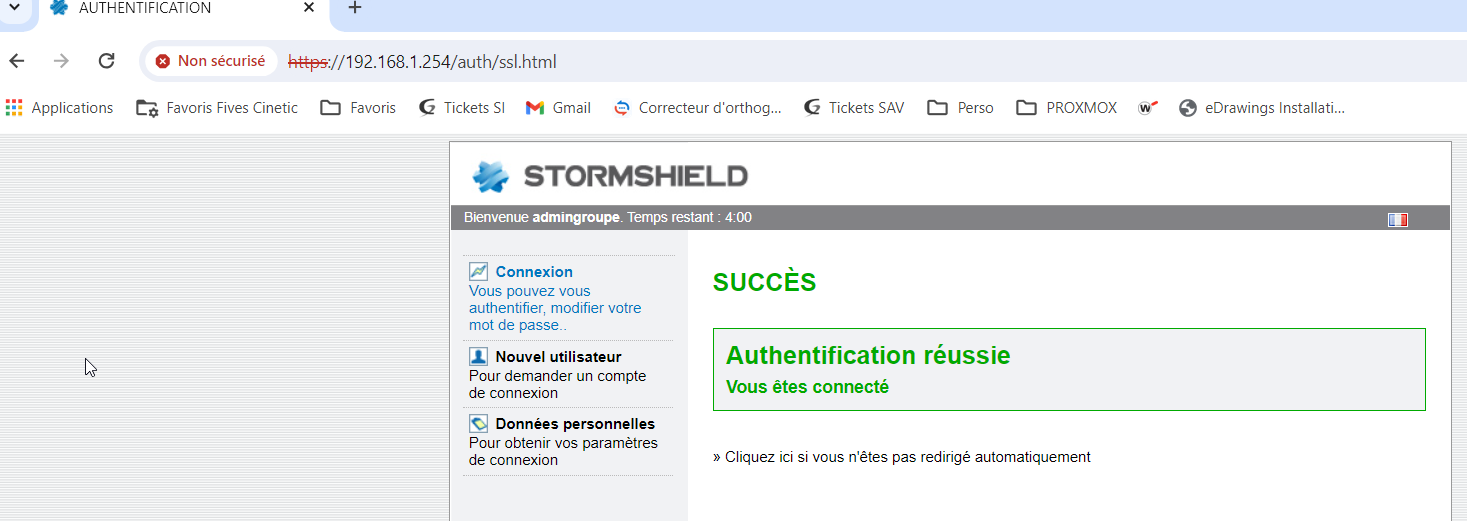
Enfin, on ajoute le certificat dans le navigateur du client



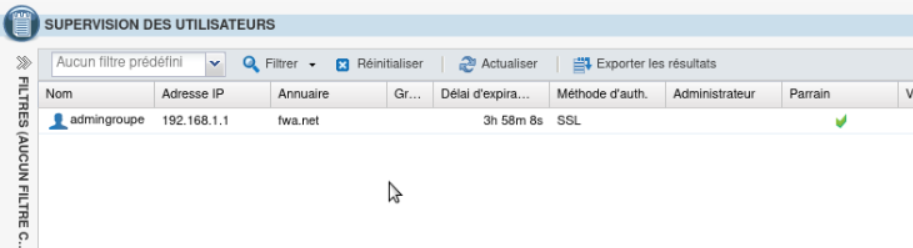
Test d’authentification :

Pour tester, je vais sur <https://192.168.1.254/auth/ssl.html> et un popup de certificat apparait

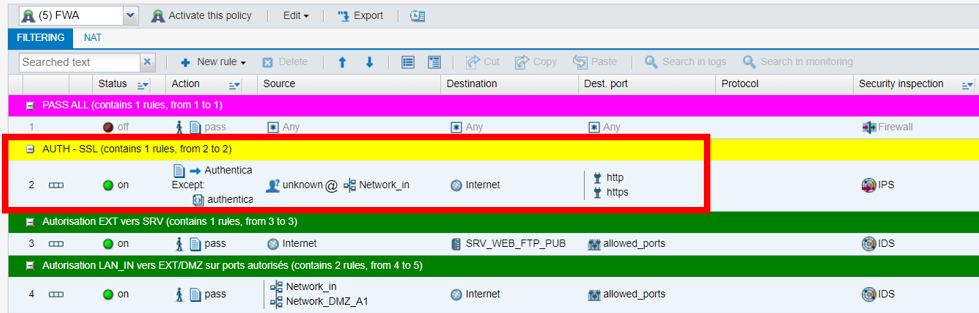


Et on obtient cela :  


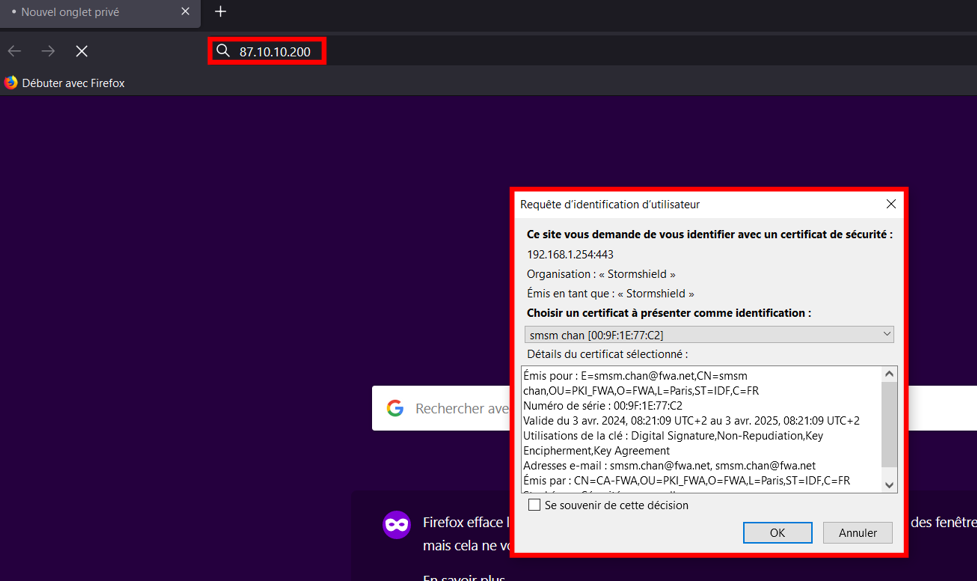
On observe que l’utilisateur est connecté :



Maintenant que la connexion est fonctionnelle en local sur le test du Stormshield, on va ajouter une règle de filtrage permettant de s’authentifier lorsqu’on fait une requête http/https



Désormais, les utilisateurs sont authentifiés lorsqu’ils vont sur un site en http/https :



Portail captif

Et plus détailler