Tâche 4 Authentification transparent par certificat SSL (9 points)

Liste des personnes impliquées avec pourcentage de répartition	
Julien : 6 point sur 9 (66,6%), Etienne : 3 point sur 9 (33,3%)	

Estimation du temps passé sur cette tâche en heure-homme :

Objectif : Mettre en place une authentification transparente pour les utilisateurs

Les firewalls implémentent plusieurs méthodes d'authentification qui peuvent être classées en deux catégories :

· Les méthodes explicites via le portail captif : l'utilisateur est redirigé vers le portail captif pour saisir un couple identifiant/mot de passe.

· Les méthodes implicites (transparentes) : l'authentification est transparente vis-à-vis de l'utilisateur qui n'a pas besoin de saisir son couple identifiant/mot de passe explicitement pour accéder au réseau.

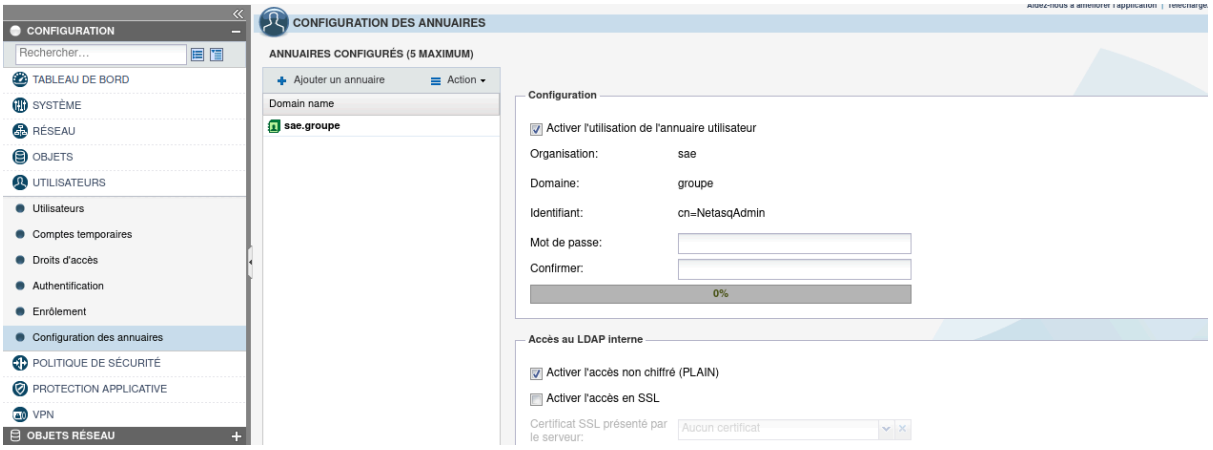
Sous-tâches	Evaluation prof
Création d'une autorité racine	
Activer l'authentification par certificat SSL	
Importez le certificat dans le navigateur	
Testez votre configuration	

Rapport

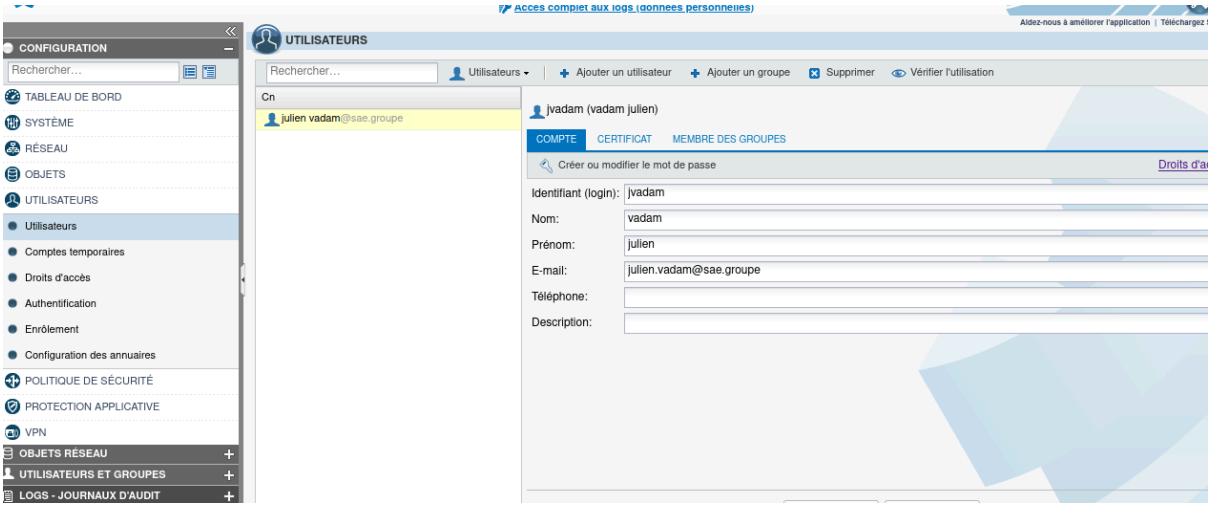
(Expliquez votre démarche, insérez les captures d'écran de votre configuration, de vos tests, etc.)

Le but de cette tâche est de réaliser une authentification sur un portail captif des utilisateurs du réseau interne qui veulent accéder au serveur externe.

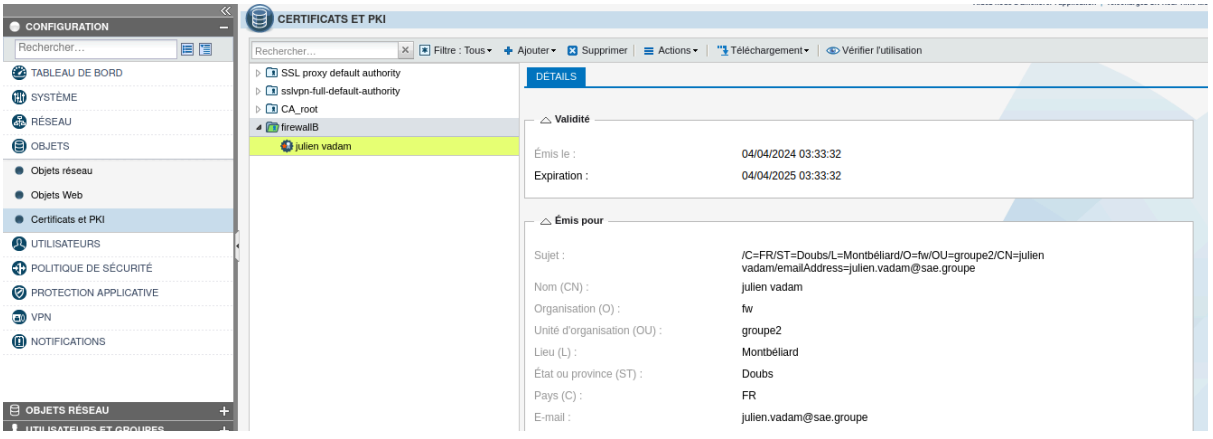
Nous avons réalisé cette authentification sur le firewall B
Afin d'activer cette authentification, il faut tout d'abord créer un annuaire LDAP interne :



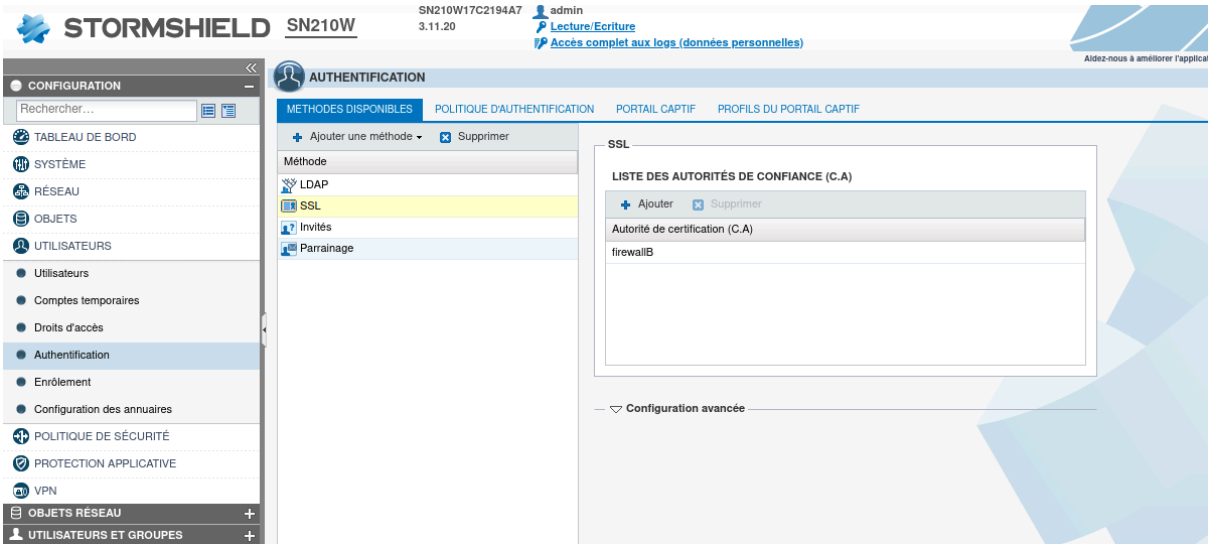
Une fois cela fait, nous avons créé dans cet annuaire un utilisateur :



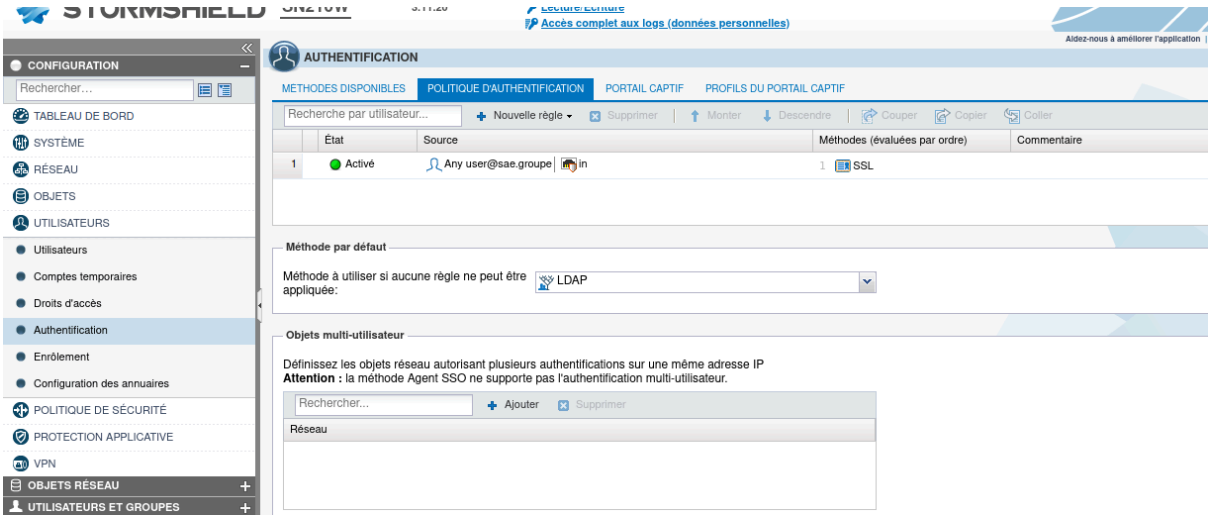
Une fois créé, nous avons ensuite ajouté une autorité de certification racine (Root-Ca). Cette autorité signe son propre certificat ainsi que les certificats utilisateurs, machines… Suite à la création de cette Root-CA, nous avons créé le certificat utilisateurs de l'utilisateur : "julien vadam".



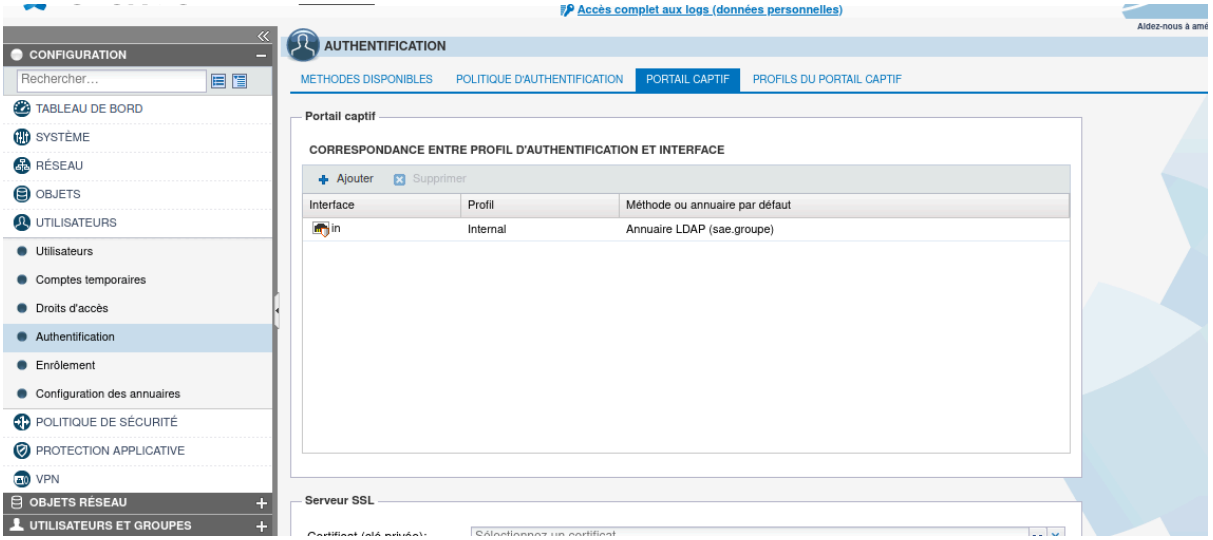
Nous avons modifié par la suite la méthode d'authentification dans le menu *Utilisateurs-> Authentification> Méthode d'authentification* en ajoutant la méthode SSL et en ajoutant en argument l'autorité de certification racine *firewallB*. Ainsi, pour chaque authentification par certificat, le stormshield ira demander à l'autorité de certification racine *firewallB* si le certificat utilisateur est valide.



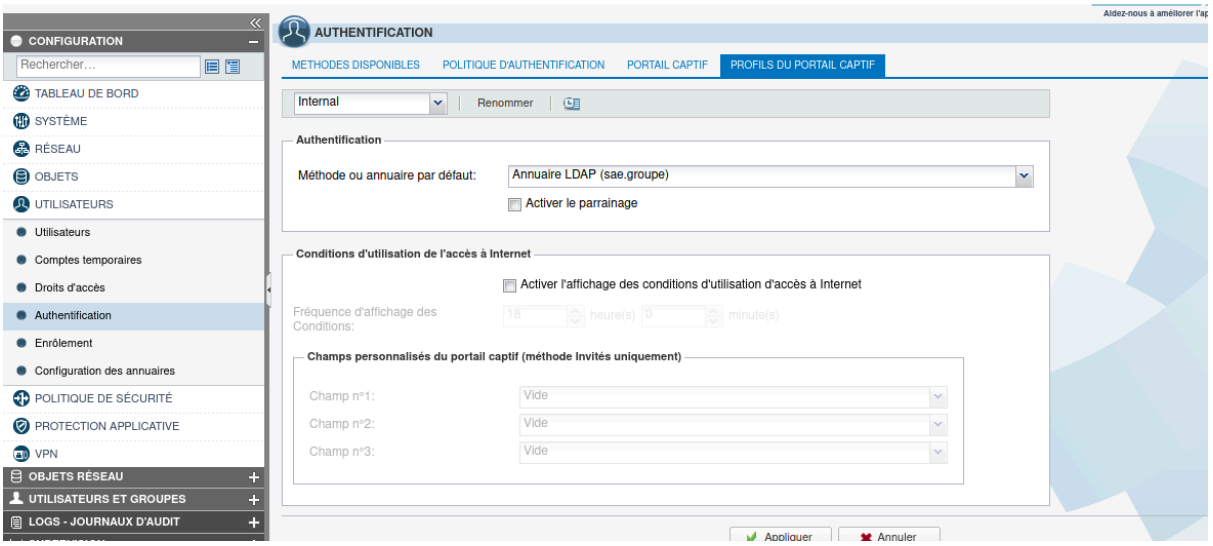
Ensuite, nous sommes allés dans le menu Politique d'Authentification et avons mis comme méthode d'authentification par défaut : SSL. J'ai également ajouté 2 règles d'authentification : L'utilisateur authuser-x sur l'interface interne du pare feu doit s'authentifier via SSL afin d'accéder à internet :



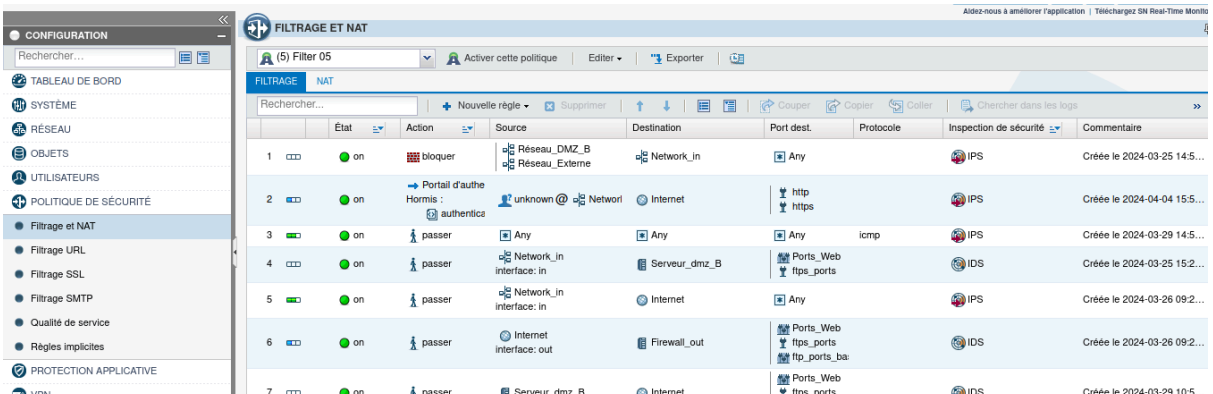
Dans l'onglet Portail Captif, nous avons ensuite ajouté une correspondance entre l'interface par laquelle les utilisateurs se connectent pour accéder à internet, soit l'interface interne du stormshield et le profil d'authentification "internal"



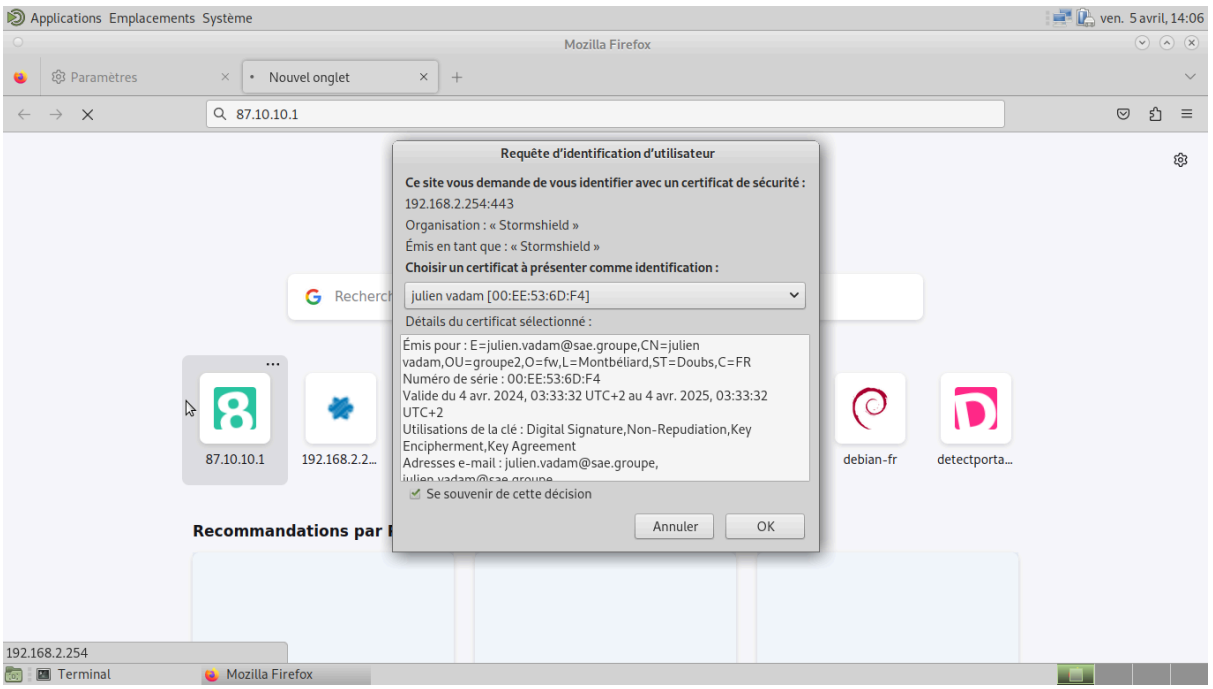
Une fois cela effectué, dans l'onglet Profil du portail captif, nous avons vérifié que la méthode par défaut où trouver les utilisateurs était l'Annuaire LDAP sae.sae



Une fois cela fait, nous avons créé une règle d'authentification dans *Politique de sécurité→ filtrage et NAT* afin que les utilisateurs non authentifiés soient redirigés vers un portail captif.



Nous pouvons vérifier que l'authentification par certificat fonctionne par cette fenêtre qui s'affiche lorsqu'on essaye d'accéder au site du pare feu A depuis le réseau interne du pare feu B :



Une fois qu'on a choisi le certificat avec lequel s'authentifier, on peut accéder à la page librement :