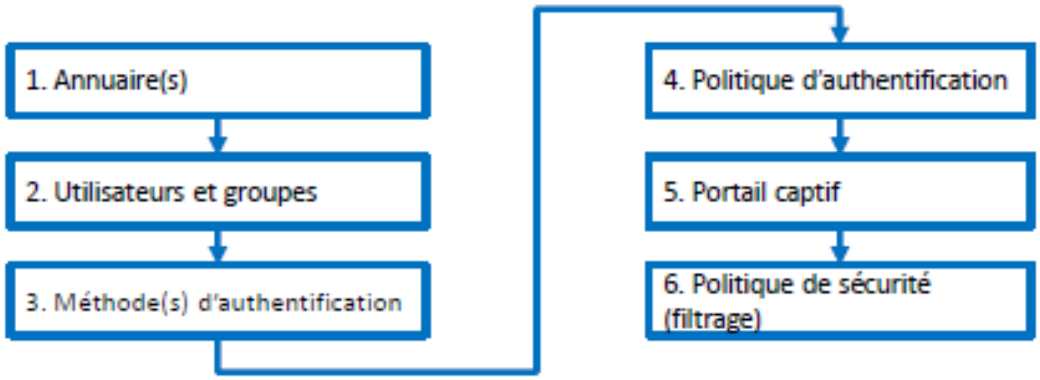
Activité 7 - Stormshield
Utilisateurs et authentification

Votre objectif

Les objectifs de l'activité sont d'accorder aux utilisateurs des droits d'accès spécifiques aux réseaux et aux services (portail captif, VPN SSL, VPN IPsec, administration du firewall, etc.)

Etapes de configuration

La gestion des droits d'accès pour les utilisateurs se définie à partir d'annuaires situés sur le firewall (c'est notre cas) ou situés sur des serveurs spécialisés comme "Active Directory" pour Microsoft.
Lors de l'activité 7 vous allez définir un annuaire interne sur le firewall SNS Stormshield. Les étapes à respecter sont :



1 - Les annuaires stockent des informations de manière hiérarchisée dans une arborescence. La norme LDAP permet l'organisation des données dans l'annuaire.

2 - Les utilisateurs sont stockés dans un annuaire et décrits par des attributs (nom, prénom, identifiant, mot de passe, adresse e-mail, certificat, etc.) utilisés par le firewall pour l'authentification.

3 - Les méthodes d'authentification utilisées permettent au firewall de configurer la façon de vérifier l'identité des utilisateurs.

4 - La politique d'authentification permet d'accorder aux utilisateurs des droits d'accès aux réseaux et services gérés par le firewall.

5 - Le portail captif peut avoir plusieurs usages : authentifier des utilisateurs pour accéder au réseau, enrôler de nouveaux utilisateurs, demander la création d'un certificat, télécharger le client VPN SSL et sa configuration, faire une demande de parrainage pour accéder au réseau, etc.

6 - La politique de sécurité contient les règles de filtrage nécessaires pour que les utilisateurs inconnus soient redirigés vers la solution d'authentification retenue (par exemple, via le portail captif).

Protocole LDAP - **L**ightweight **D**irectory **A**ccess **P**rotocol
Ce protocole est utilisé pour accéder et maintenir des services d'annuaire distribués sur un réseau. Les annuaires LDAP sont souvent utilisés pour stocker des informations sur les utilisateurs, les groupes et les ressources dans un environnement réseau.

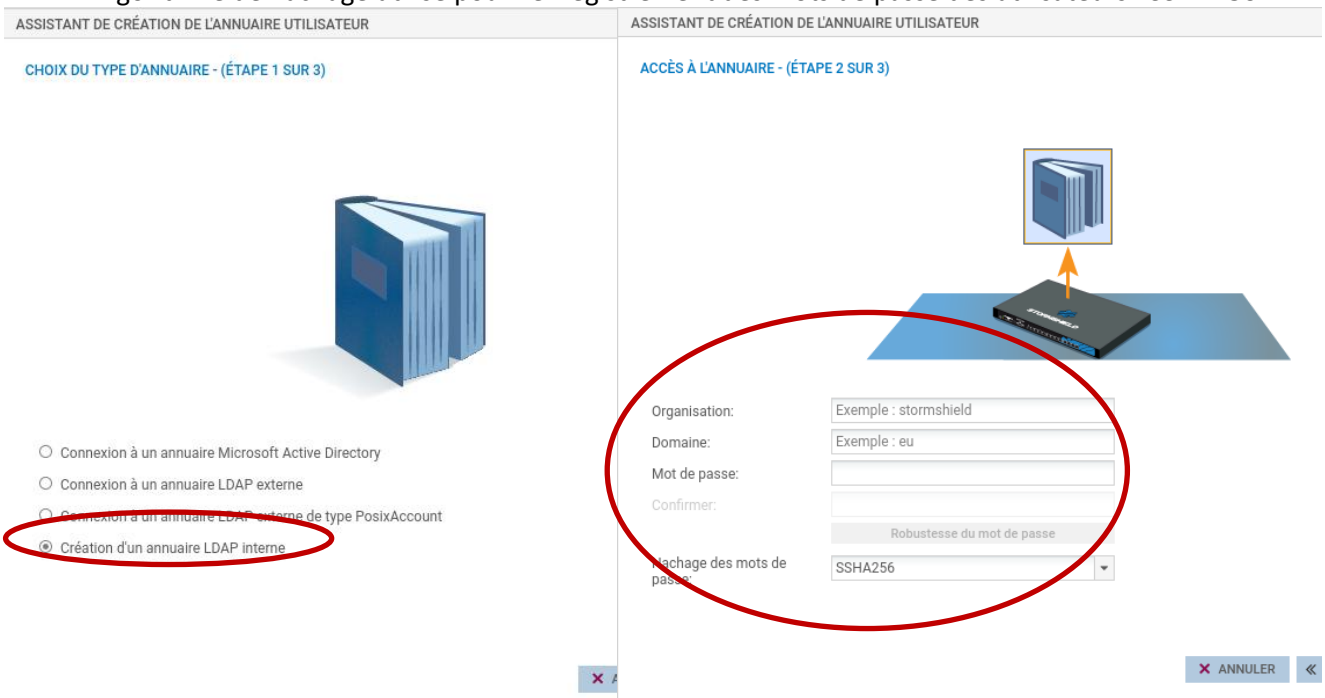
Dans notre cas, nous utiliserons un annuaire hébergé sur le pare-feu. On parle d'annuaire interne.

Configurer la liaison à un annuaire

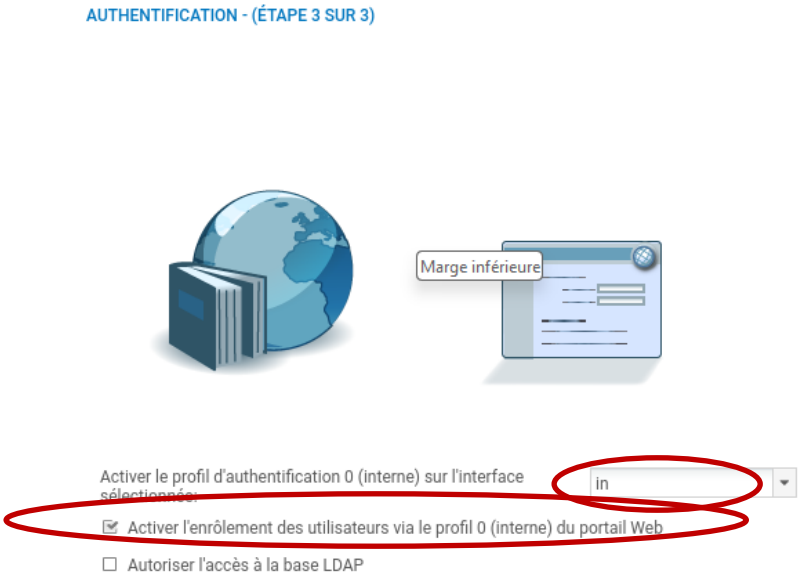
☞ 1 – Copiez la politique de filtrage/NAT **(6) Activite_6** vers la politique numéro 7. Renommez la politique "**Activite_7**", puis activez cette politique (bouton "**Appliquer**" en bas de la page).

☞ 2 – Pour utiliser un annuaire LDAP interne, lancez l'assistant de configuration LDAP.
Pour cela, allez dans le menu **Configuration => Utilisateurs => Configuration des annuaires**.
Cliquez sur ajouter un annuaire.

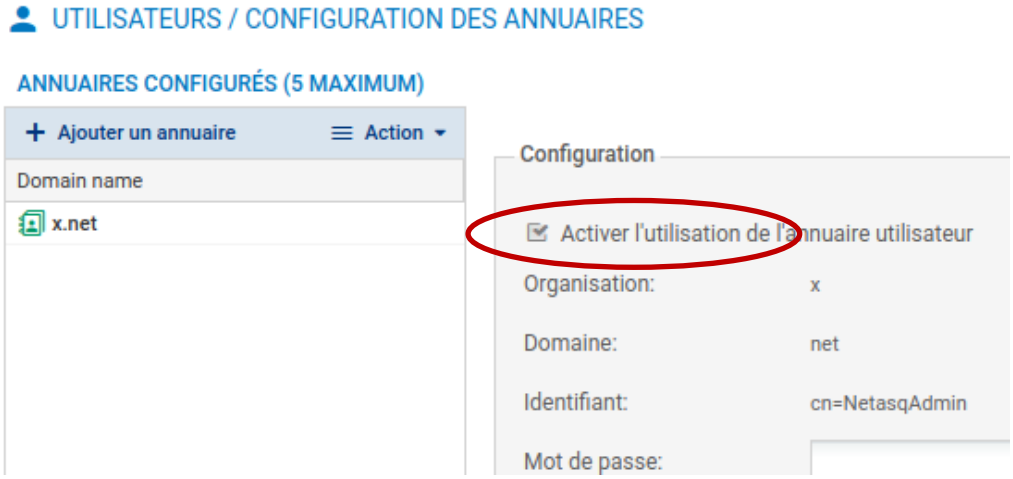
☞ 3 – Choisissez l'option **Annuaire LDAP interne**, et renseignez les champs demandés :
- Organisation : **x**
- Domaine : **net**
- Mot de passe pour se connecter à l'annuaire : **MonAnnuaire**
- Algorithme de hachage utilisé pour l'enregistrement des mots de passe des utilisateurs : **SSHA256**



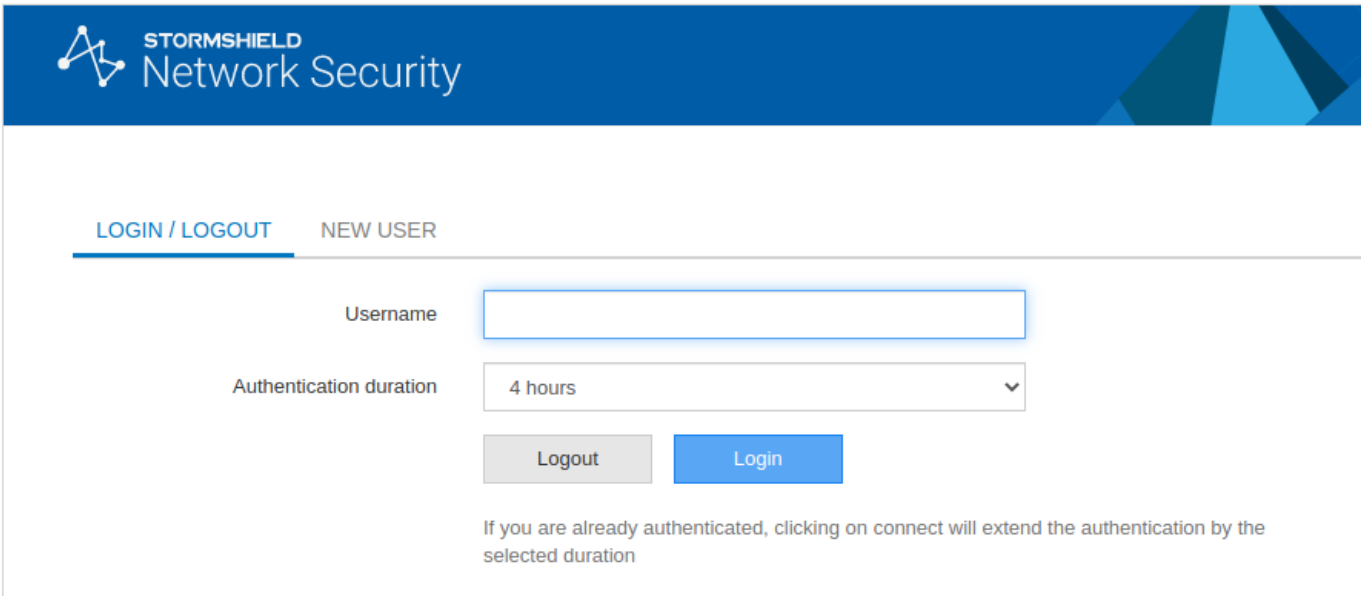
☞ 4 – A l'étape suivante, choisissez l'interface **in** pour le profil 0 et pensez à activer l'enrôlement des utilisateurs pour ce profil.
L'enrôlement des utilisateurs permet aux utilisateurs qui ne sont pas présents dans l'annuaire de remplir un formulaire de création de compte qui sera soumis à l'approbation de l'administrateur.



☞ 5 – Vérifiez que le service est activé



☞ 6 – Testez l'accès au portail captif par https://192.168.1.254/auth .

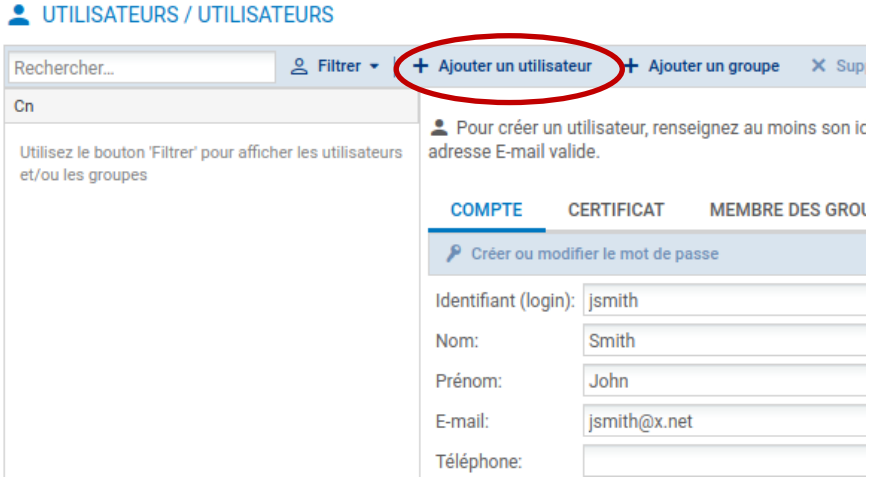


Gestion des utilisateurs

☞ 7 – Créez un utilisateur John Smith :

- Identifiant : **jsmith**
- Mot de passe : **password**
- Adresse email : jsmith@x.net

Vous devez vous rendre dans le menu **Configuration => Utilisateurs => Utilisateurs**, cliquez sur **Ajouter un utilisateur**.



☞ 8 – Apres validation, vous devez préciser le mot de passe pour le compte de John Smith.

Mot de passe : **mdpsmith**

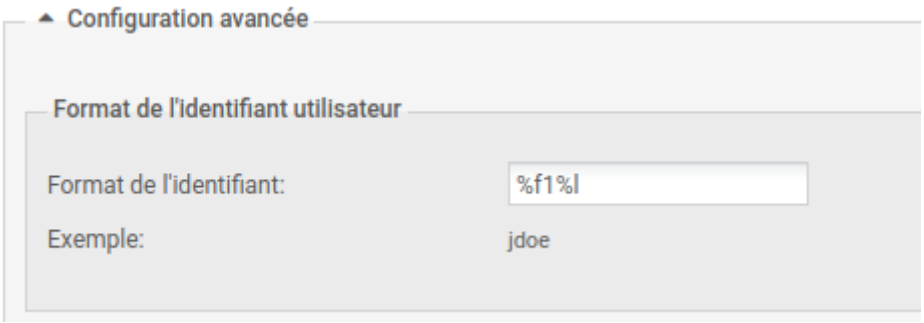
Cette méthode suppose que l'administrateur possède la liste de les employés de l'entreprise (ce qui doit être le cas) mais certains employés qui "sont de passage" (stagiaires, intérimaires, visiteurs …). Pour ne pas perdre trop de temps dans la création de ces compte temporaires, on utilise la méthode de "l'enrolement".
L'utilisateur va compléter un formulaire accessible depuis le portail Captif pour faire une demande d'accès qui devra être validée par l'administrateur.

☞ 9 – Utilisation de la fonction d'enrôlement pour créer automatiquement un utilisateur.

Sur le firewall, rendez-vous dans la section **Configuration => Utilisateurs => Enrôlement => Configuration avancée**, pour changer le format par défaut de l'identifiant en tapant **%f1%l** .
On peut définir automatiquement le format de l'identifiant à partir des infos saisies depuis le formulaire.
Prenons le cas de l'utilisateur Peter Wood :

- **%F.%L :** Donne **PETER.WOOD** (F pour FIRSTNAME et L pour LASTNAME)**.**
- **%f1.%l :** Donne **p.wood** (première lettre du prénom en minuscule, point, et nom en minuscules).
- **%f%L1** : Donne **peterW** (prénom en minuscules, première lettre du nom en majuscule).

Dans notre cas, **%f1.%l** donnera **p.wood**

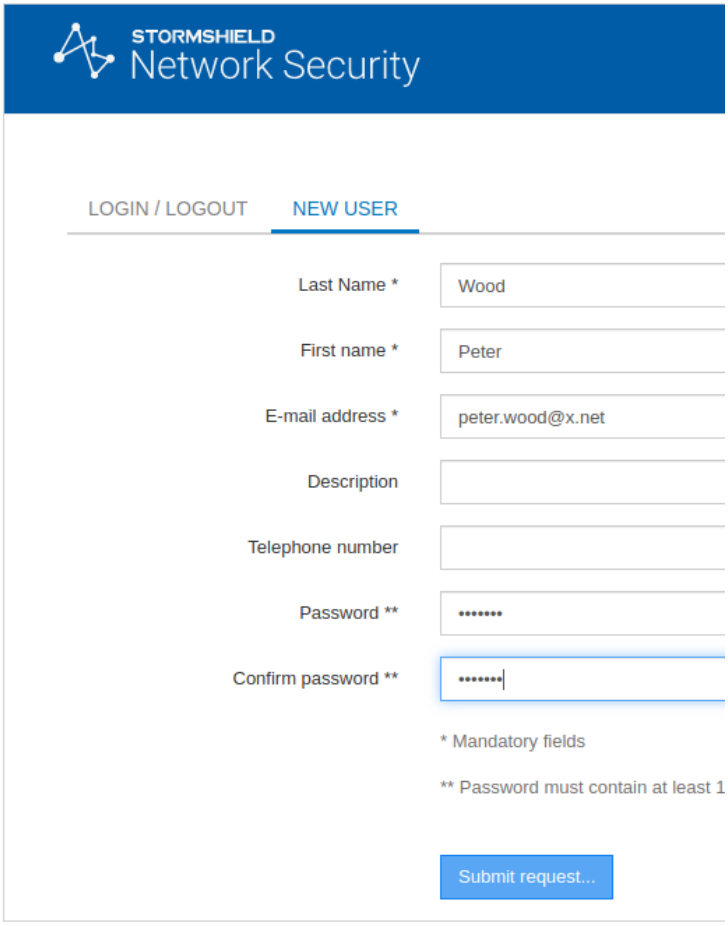


N'oubliez pas de cliquer sur "Appliquer".

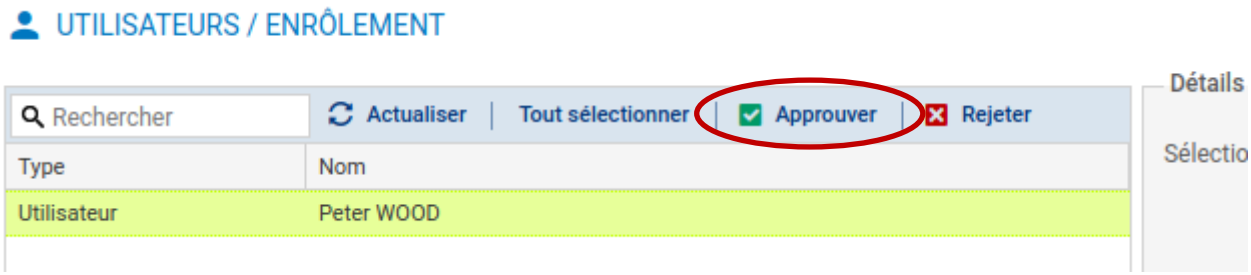
☞ 10 – Connectez-vous au portail captif https://192.168.x.254/auth puis cliquez sur l'onglet **Nouvel Utilisateur**.

Remplissez le formulaire avec les informations nécessaires (utilisateur **Peter Wood** / Mot de passe **mdppetermdwood**) puis validez.

Validez la modification puis cochez la demande de l'utilisateur Peter Wood et cliquez sur Valider.



☞ 11 – Vérifiez si la demande est bien présente au niveau du firewall dans le menu **CONFIGURATION ⇒ UTILISATEURS ⇒ Enrôlement**. L'administrateur peut sélectionner l'utilisateur par un double clic, puis approuver, rejeter ou ignorer la demande. En cas d'approbation, l'identifiant (login) de l'utilisateur est généré automatiquement selon le format choisi à l'étape précédente.
Validez la demande de l'utilisateur Peter Wood.



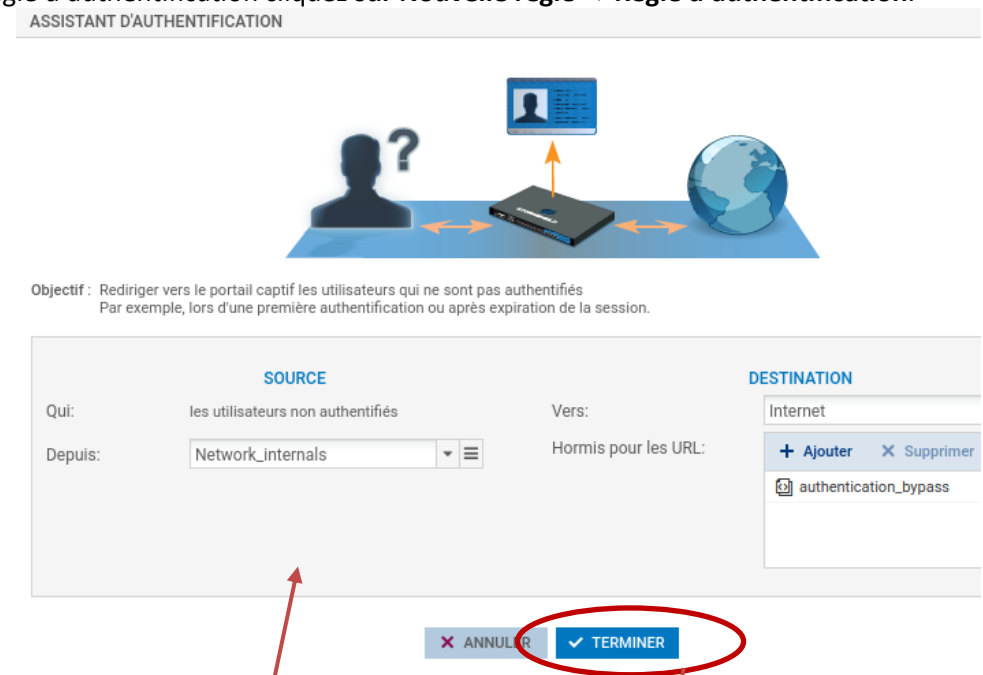
☞ 12 – Testez l'authentification de chacun des utilisateurs (John et Peter) depuis le portail captif.

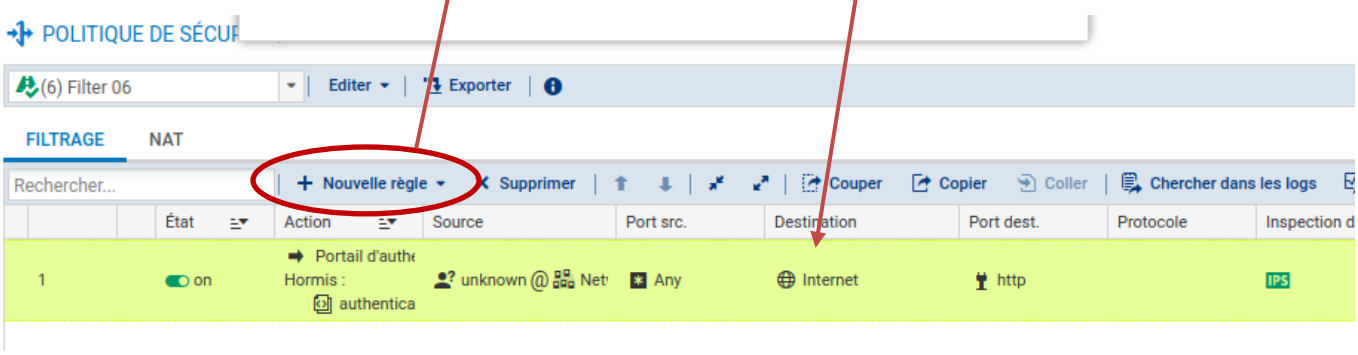
Politique de sécurité

☞ 13 – Par sécurité, on veut que tous les utilisateurs non authentifiés soient redirigés vers le portail captif lorsqu'ils tentent d'accéder à des sites WEB en HTTP, sauf les sites présents dans la catégorie **it**.
Pour cela, il faudra ajouter une règle d'authentification avant la règle actuelle pour HTTP, qui contiendra :

PASS (+redirection vers le service authentification) from unknown users@Network_in to Internet (service http) + Exception pour le groupe IT.

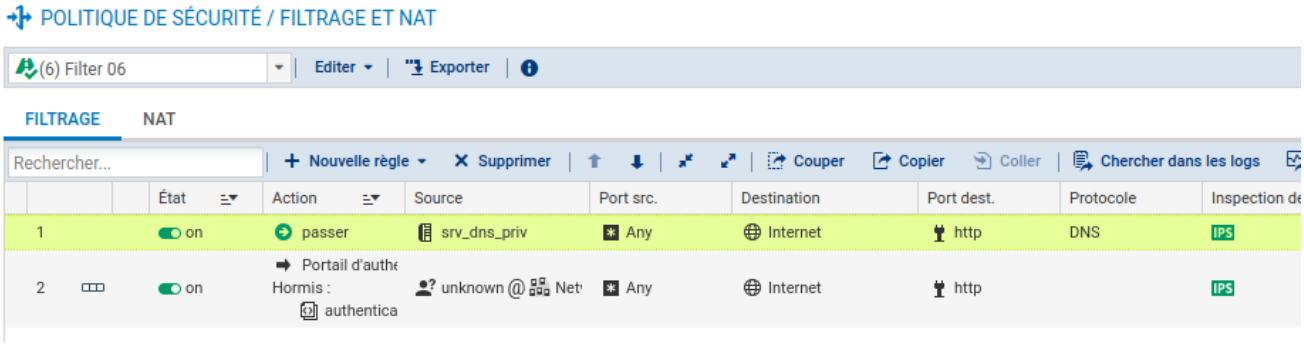
Pour créer la règle d'authentification cliquez **sur Nouvelle règle ⇒ Règle d'authentification**.





ATTENTION

Avant d'ajouter cette règle, il faut s'assurer que les connexions DNS sont autorisées pour tous les utilisateurs (authentifiés ou non), car sans résolution DNS, il n'y aura pas de requêtes HTTP et par conséquent, pas de redirection vers le portail captif.



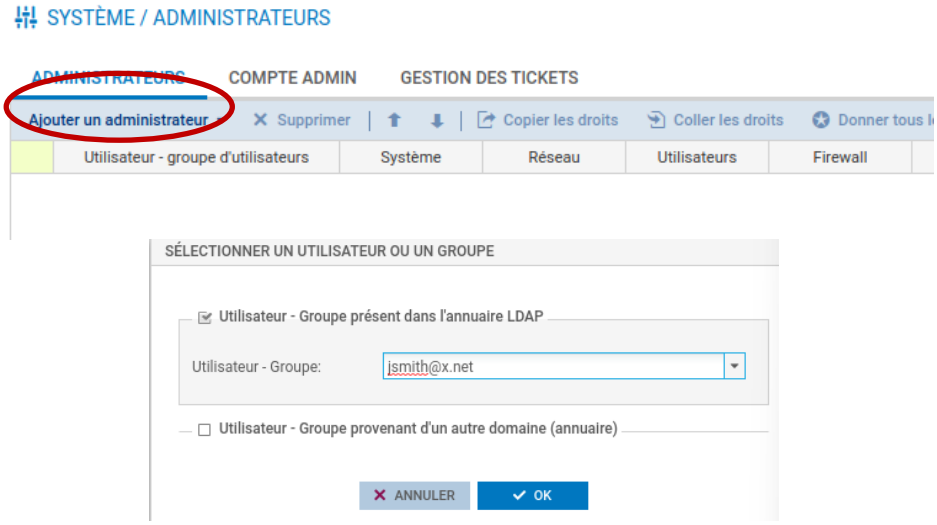
☞ 14 – (Manip difficile à faire à la fin de l'activité) Exclure de cette règle les sites de la catégorie "**IT**".

Il faudra créer une nouvelle règle et la positionnée avant la règle sur les utilisateurs non authentifiés. Cette règle autorisera l'accès de tous les utilisateurs à seulement la catégorie "IT". Vous devrez aussi définir un filtrage d'URL et associer ce filtrage à la règle.

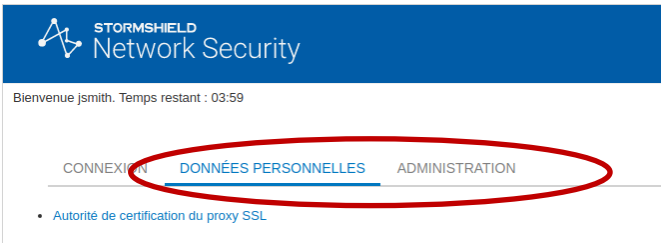
Depuis un navigateur, accédez à un site IT en HTTP (http://netbsd.org par exemple), puis essayez d'accéder à un autre site en HTTP ne relevant pas de cette catégorie (http://neverssl.org par exemple).
Le portail captif devrait alors apparaître automatiquement.

☞ 15 – Donnez à John Smith les droits de supervision sur le Firewall.

Dans le menu Configuration => Système => Administrateurs, ajoutez une entrée pour l'utilisateur jsmith en lui donnant les droits de supervision (administrateur avec accès aux données personnelles) et validez.



☞ 16 – Connectez-vous sur le firewall avec le compte **jsmith** et validez l'accès aux différents menus de supervision. Testez également l'authentification avec ce compte sur le portail captif d'authentification.



☞ 17 – BONNUS - Modifiez la politique de filtrage pour que l'envoi de pings depuis votre réseau interne ne soit autorisé qu'à John Smith. Cette règle devra systématiquement lever une alarme mineure.