POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

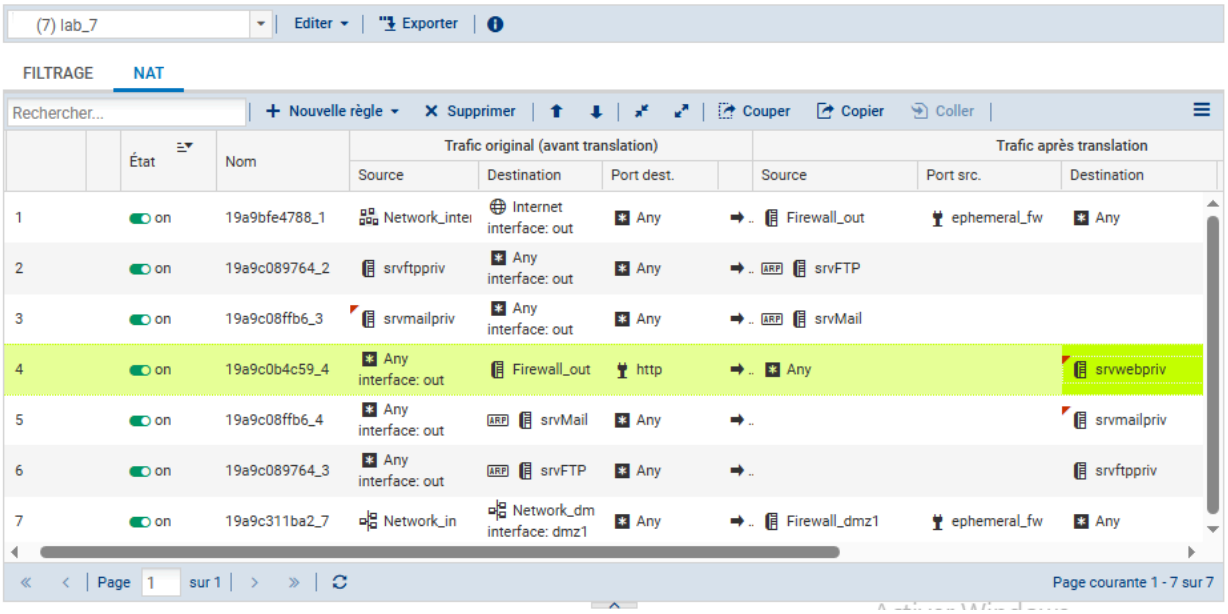
(7) lab_7 | Editer | Exporter

FILTRAGE NAT

Rechercher... | Nouvelle règle | Supprimer | Couper | Copier | Coller

	Nom	État	Action	Source	Destination	Port dest.	Protoc...	Inspection de sécurité
NetIN to Internet (contient 9 règles, de 2 à 10)								
2	19a9c700796_2	on	bloquer	Network_in	Internet geo Corée du Sud	http https		IPS
3	19a9c7ed542_4	on	bloquer	Network_in	FQDN www.cnn.com	https		IPS
4	19a9c8425c1_5	on	bloquer	PC_200	Any	ftp		IPS
5	19a9c8a3018_5	on	passer	Network_in	Network_out	ssh		IPS
6	19a9c95641f_6	on	passer	srvdnspriv	Any	dns		IPS
7	19a9c82655a_4	on	passer	Network_in	Internet	ftp		IPS
8	19a9c877b3c_6	on	passer	Network_in	Any	Any	icmp	IPS
9	19a9c745a47_3	on	passer	Network_in	Internet	http https		IPS
10	19aa01cd667_a	on	passer	srvmailpriv	Any	smtp		IPS
Internet to DMZ (contient 5 règles, de 11 à 15)								
11	19aa0247952_c	on	passer	Network_out	srvFTP	ftp		IPS
12	19aa01f6264_b	on	passer	Network_out	Firewall_out	http		IPS
13	19aa02aa656_d	on	passer	Network_out	srvMail	smtp		IPS
14	19aa02c3d37_e	on	passer	Network_out	Firewall_out	Any	icmp	IPS
15	19aa02eaac1_f	on	passer	Network_out	Firewall_out	ssh https		IPS
NETint to DMz (contient 1 règles, de 1 à 1)								
1	19a9c63f0a4_1	on	passer	Network_in	Network_dmz1	dns http weba ftp smtp		IPS

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT



Lab 7 - Authentification

Copiez la politique de filtrage/NAT (6) Lab*6 vers la politique numéro 7. Renommez la politique numéro 7 « Lab7* », puis activez cette politique.

1. Lancez l'assistant LDAP et créez une base LDAP interne :

- Le nom d'organisation est x, et le domaine est « net ».
- Activez le profil d'authentification 0 (internal) sur l'interface « IN », ainsi que l'enrôlement des utilisateurs.
- Testez l'accès au portail captif : https://192.168.x.254/auth

1. Créez un utilisateur John Smith :

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

1. En utilisant la fonction d'enrôlement, créez un utilisateur « Peter Wood » avec le mot de passe : password
2. Testez l'authentification de chacun des utilisateurs.
3. 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.
4. Adaptez la politique de filtrage afin 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 ».
5. Tester l'accès en HTTP à un site appartenant à la catégorie « it » et confirmer la redirection vers le portail pour tout autre site en HTTP n'appartenant pas à cette catégorie.
6. Donnez à John Smith les droits de supervision sur le Firewall.
7. Connectez-vous sur le firewall avec le compte « jsmith » et validez l'accès aux différents menus. Testez également l'authentification avec ce compte sur le portail d'authentification.

Étape 1 : Préparation de l'environnement (Politique)

Pourquoi ? Comme toujours, on ne travaille jamais sans filet de sécurité (backup) et on itère sur une base saine. On conserve le Lab 6 fonctionnel au cas où.

Action :

1. Allez dans **POLITIQUE DE SÉCURITÉ > Filtrage et NAT**.
2. Sélectionnez `(6) Lab6`.
3. Cliquez sur **Copier**, puis **Coller**.
4. Renommez la copie `(7) Lab7`.
5. Cliquez sur **Activer cette politique**.

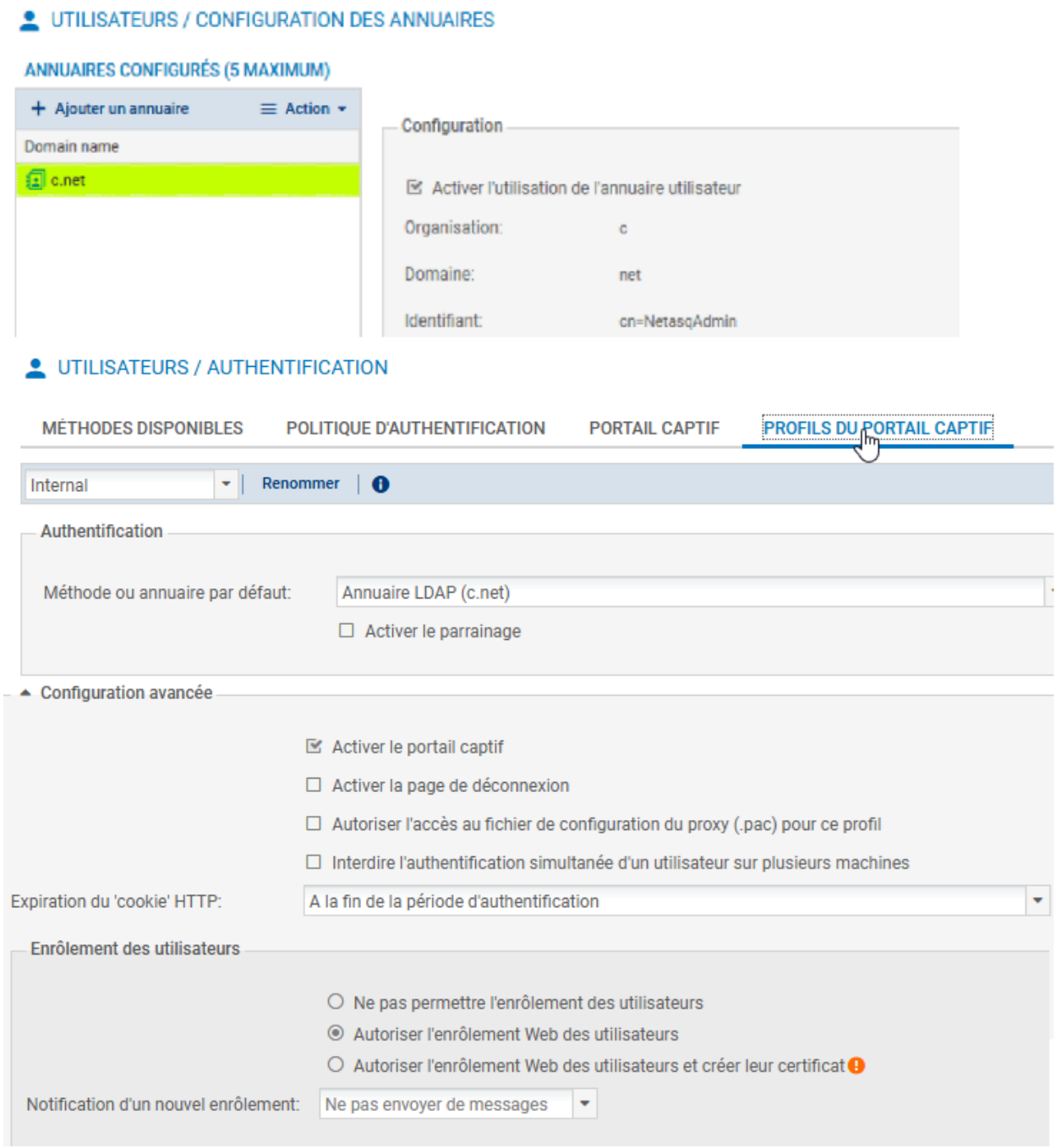
Étape 2 : Création de l'Annuaire (LDAP Interne)

Pourquoi ? Pour authentifier des utilisateurs, le pare-feu a besoin d'une base de données. Ici, nous allons utiliser la base **Interne** du Stormshield (idéal pour les PME ou les labs). Nous allons aussi lier cette base à une interface réseau pour que le pare-feu sache "où" écouter les demandes d'authentification.

Action :

1. Allez dans **CONFIGURATION > UTILISATEURS > Configuration de l'annuaire**.
2. Cliquez sur **Ajouter un annuaire**.
3. Choisissez **Connect to an internal LDAP directory** (Créer un annuaire LDAP interne). Suivant.
4. Remplissez les champs :
    - **Organisation :** `c` (Remplace `c` par ton trigramme ou numéro de stagiaire si nécessaire, sinon mets juste `c`).
    - **Domaine :** `net` (Ce qui donnera des utilisateurs du type `user@c.net`).

    - **Mot de passe :** `password` (ou celui de ton choix, c'est pour l'admin LDAP).
5. Cliquez sur **Suivant**.
6. **Liaison Interface :** L'assistant vous demande sur quelle interface activer le profil 0. Sélectionnez votre interface **Internal** (souvent `in` ou `dmz1` selon ton plan d'adressage, ici le lab semble indiquer le réseau interne).
7. **Cochez impérativement** la case : `Activer l'enrôlement des utilisateurs...` (Enable user enrollment).
8. Terminez l'assistant.

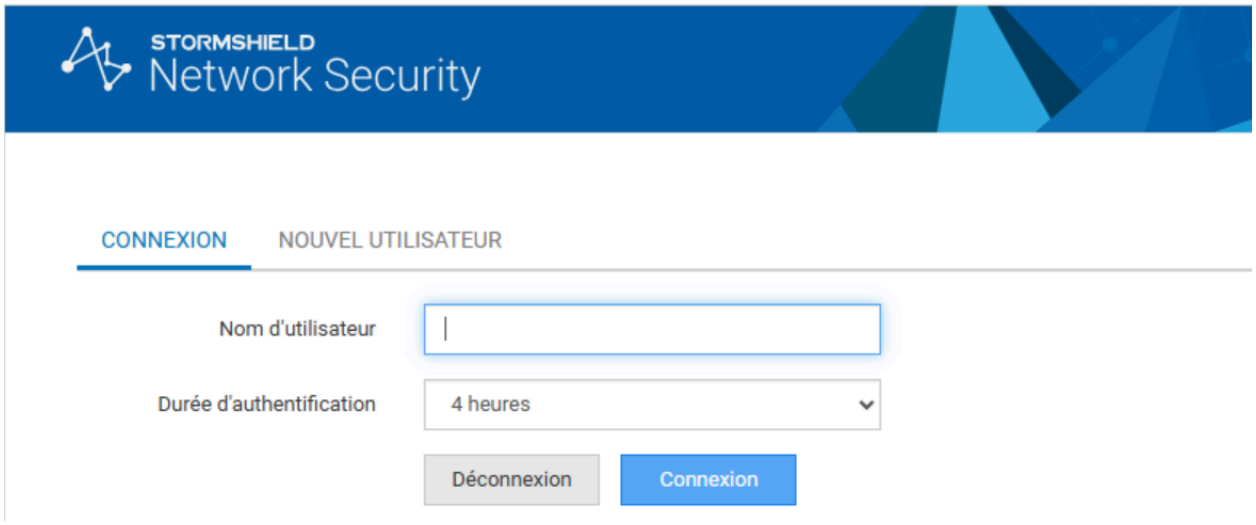


Étape 3 : Test du Portail Captif

Pourquoi ? On vérifie que le service Web d'authentification (le daemon) tourne bien avant d'essayer de loguer des gens.

Action :

- Depuis ta machine virtuelle cliente (Windows/Linux dans le LAN), ouvre un navigateur.
- Va sur : `https://192.168.3.253/auth` (ton sous-réseau)
- Tu dois voir la page de connexion bleue Stormshield. (Accepte l'avertissement de certificat, c'est normal).



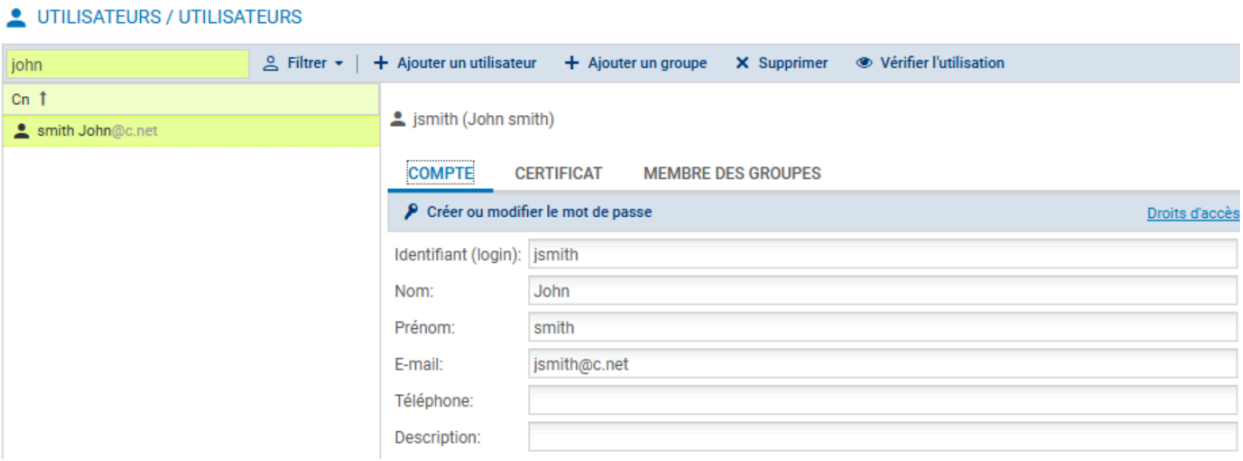
Étape 4 : Création manuelle d'un utilisateur (John Smith)

Pourquoi ? On crée un compte "standard" pour tester les droits spécifiques plus tard.

Action :

1. Allez dans **CONFIGURATION > UTILISATEURS > Utilisateurs**.
2. Cliquez sur **Ajouter un utilisateur**.
3. Remplissez la fiche :
    - **Identifiant (Login) :** `jsmith`
    - **Nom :** Smith
    - **Prénom :** John
    - **Email :** `jsmith@x.net`

4. Cliquez sur **Appliquer**.
5. Une popup s'ouvre pour définir le mot de passe. Mets : `password`.

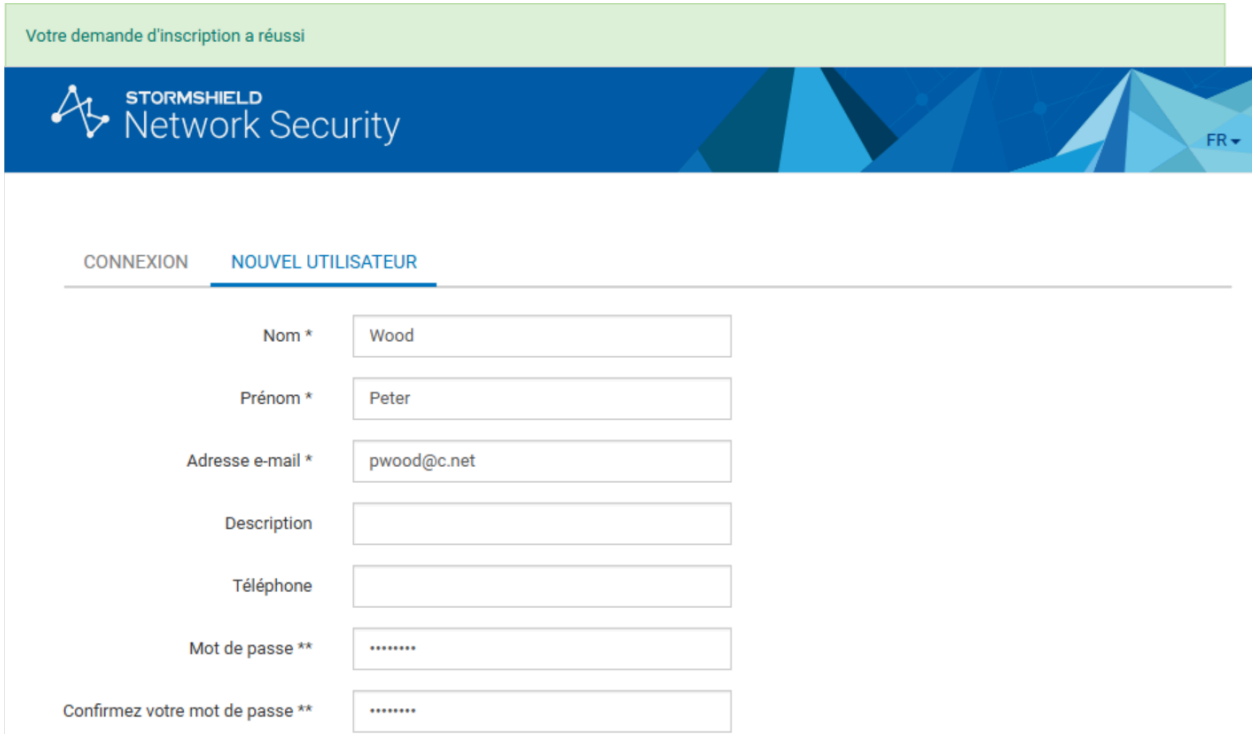


Étape 5 : Enrôlement d'un utilisateur (Peter Wood)

Pourquoi ? L'enrôlement permet aux utilisateurs (ex: invités, consultants) de créer eux-mêmes leur compte via le portail. C'est du "Self-Service".

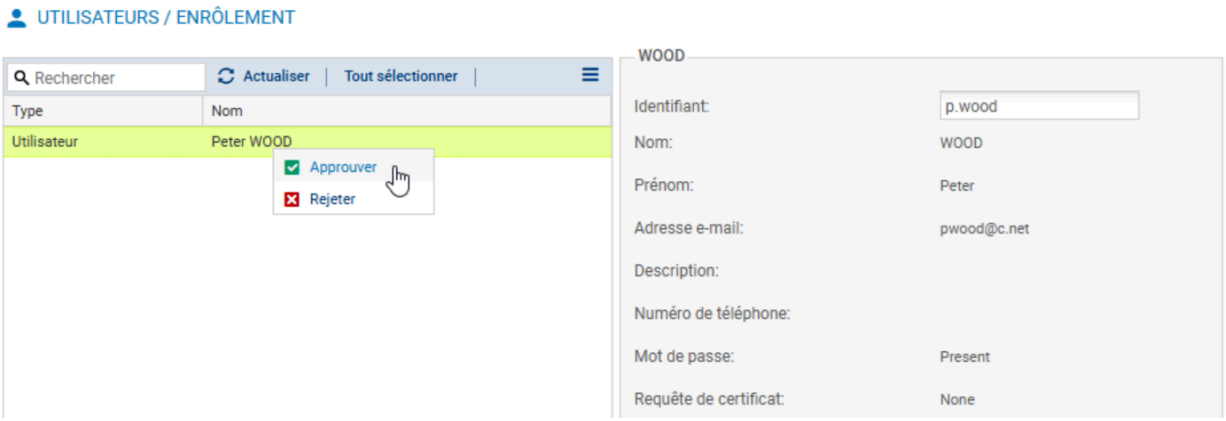
Action (Côté Utilisateur) :

1. Retourne sur le navigateur du client (`/auth`).
2. Clique sur le lien/bouton **"Nouvel utilisateur"** (New User).
3. Remplis le formulaire pour **Peter Wood** (Email: `pwood@x.net`, Mot de passe: `password`).
4. Valide. Tu auras un message disant que la demande est soumise.



Action (Côté Administrateur - CRUCIAL) : *L'utilisateur n'est pas créé tant que l'admin ne valide pas !*

1. Sur le Firewall, va dans **CONFIGURATION > UTILISATEURS > Enrôlement**.
2. Tu dois voir la demande de Peter Wood.
3. Sélectionne la ligne et clique sur **Approuver** (Approve).
4. Vérifie que son login généré te convient (souvent `p.wood` ou `peter.wood` selon le format par défaut). Valide.



Test : Connecte-toi sur le portail avec `jsmith` puis `pwood` pour vérifier que les deux fonctionnent.

Étape 6 : Filtrage Identitaire (Le Ping pour John)

Pourquoi ? On va prouver qu'on peut filtrer par identité. On veut que *seul* John puisse pinger, pas Peter, ni personne d'autre.

Action :

1. Allez dans **POLITIQUE DE SÉCURITÉ > Filtrage et NAT**.
2. Ajoutez une règle en haut (avant les règles "pass all").
3. **Action :** `Passer`
4. **Source :** `Any`. (network_in ça marche pas !)
5. **Utilisateur :** Double-clique dans la colonne source sur l'icône utilisateur. Cherche et sélectionne `John Smith` (ou `jsmith`).
    - *Résultat visuel :* `jsmith` (dans la case, regarder image en bas)
6. **Destination :** `Any`.
7. **Protocole :** `icmp` (Ping).
8. **Alarme :** Dans la colonne "Action", double-clique pour éditer. Change "Alarme" de "Aucune" à **"Mineure"**.
9. **Appliquer**.

Test : Connecte-toi au portail avec John Smith, essaie de pinger 8.8.8.8 (ça marche). Déconnecte-toi (Logout), connecte Peter Wood, ping (ça doit bloquer, sauf si tu as une règle "Pass All" en dessous qui laisse passer le ping pour tout le monde).*

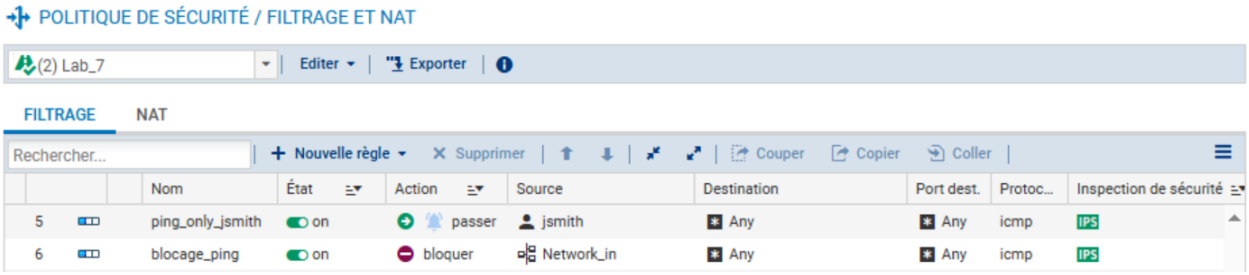
Vu que j'ai une règle de pass all pour le ping en dessous et je veux pas l'enlever j'ai créé une règle pour bloquer tout le monde (sauf jsmith avec la regle au dessus) :
Action : **`Bloquer`**

Source : `Any` (ou `Network_in`)

Utilisateur : `Any` (Tout le monde)

Destination : `Any`

Protocole : **`icmp`** (Ping)



Comme ça, dès que je suis logué et authentifié avec jsmith le ping fonctionne mais avec pwood no fonctionne pas (le lab me demandait de faire ça).

1. **Règle 5 (Spécifique) :** Autorise `jsmith` (depuis n'importe où) à pinger.
2. **Règle 6 (Générique) :** Bloque le reste du réseau interne pour le ping.

💡 Le point clé que tu as découvert (Admin vs Auth)

C'est la nuance la plus importante de ce Lab :

- **Session Admin (`/admin`) :** C'est juste un droit d'accès à l'interface de gestion (couche Application). Ça ne change rien à ton adresse IP pour le moteur de filtrage.
- **Session Portail (`/auth`) :** C'est celle qui dit au moteur de filtrage (ASQ) : *"L'adresse IP `192.168.3.x` appartient maintenant à `jsmith`"*. C'est **celle-ci** qui active la Règle 5.

Étape 7 & 8 : Règle d'Authentification (HTTP) & Exception

Pourquoi ? C'est le cœur du sujet. On veut forcer l'authentification (Redirection Portail) pour aller sur le Web, MAIS on veut laisser l'accès libre (Transparent) aux sites de la catégorie "IT" (ex: pour que les admins accèdent aux docs techniques sans se loguer).

Action :

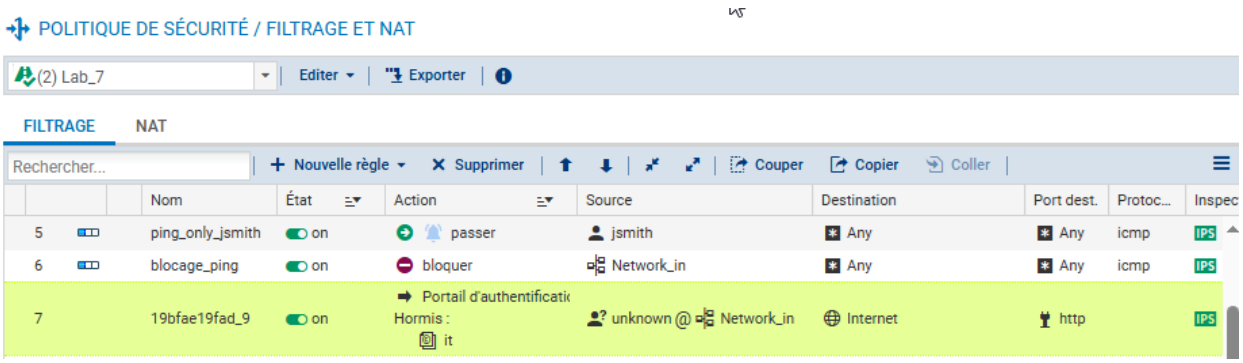
1. Dans la politique de filtrage, clique sur la flèche à côté de **Nouvelle règle** et choisis **Règle d'authentification**.
2. L'assistant se lance :
    - **Utilisateur :** `Utilisateurs inconnus` (Unknown users).
    - **Source :** `Network_in`.
    - **Destination :** `Internet` (ou Any).
    - **Service :** `http` (Le portail captif ne marche bien qu'en HTTP pour la redirection initiale).
    - **Rediriger vers :** `Portail captif`.
3. **L'Exception ("IT") :**
    - Soit l'assistant te propose une case "Excepté pour les URL...", sélectionne la catégorie `it`.
    - Soit (plus robuste), une fois la règle créée, ajoute une règle standard **Passer** juste **AU-DESSUS** de la règle d'auth :
        1. Action: `Passer`
        2. Source: `Network_in`
        3. Dest: `Internet`
        4. Port: `http` (Important : ne mets pas HTTPS car le portail captif ne redirige que le HTTP standard)
        5. **Filtrage URL :** Crée un profil URL qui autorise *uniquement* la catégorie `it` et bloque le reste ? **Non**, plus simple :

- *Méthode recommandée Stormshield :* Dans la règle d'authentification elle-même, double-clique. Cherche l'option "Destination exemptées d'authentification" ou similaire si dispo.
- *Méthode "Règles" (Classique) :*
    1. Règle 1 : **Passer** | Source: Any | Dest: Internet | Port: http | **URL Filter: Allow_IT_Only** (Profil qui laisse passer IT). -> *Les utilisateurs inconnus peuvent passer ici.*
    2. Règle 2 : **Auth (Portail)** | Source: Any | Dest: Internet | Port: http. *-> Les autres se font attraper ici.*

Note : La consigne dit "Rediriger... sauf IT". La méthode la plus propre sur SNS est souvent de mettre une règle "Passer" vers la catégorie URL "it" ***avant*** *la règle d'authentification.*

Action Concrète :

1. Créez une règle N°1 : **Passer** | Source : `Network_in` | Dest : `Any` | Port : `http` | Filtrage URL : (Crée un profil qui a juste `it` en "passer" et rien d'autre).
2. Créez une règle N°2 (Auth) : **Authentification** | Source : `Network_in` (Unknown) | Dest : `Any` | Port : `http`.



Étape 9 : Test HTTP

1. **Sans être authentifié** (déconnecte-toi du portail via `/auth` bouton Logout).
2. Tente d'aller sur `http://www.netbsd.org` (Site IT). -> **Ça doit passer sans demander de login. OUI!**
3. Tente d'aller sur `http://www.lemonde.fr` (News). -> **Tu dois être redirigé vers le portail bleu. OUI!**

Étape 10 : Droits d'administration pour John

Pourquoi ? On veut déléguer la surveillance à John sans lui donner les clés de toute la configuration (Principe de moindre privilège).

Action :

1. Allez dans **CONFIGURATION > SYSTÈME > Administrateurs**.
2. Onglet **Administrateurs**.
3. Cliquez sur **Ajouter un administrateur**.
4. Sélectionnez l'utilisateur `jsmith` dans la liste.
5. Dans la colonne des droits, choisissez un profil restreint, par exemple **"Administrateur avec accès en lecture seule"** ou cochez manuellement les cases pour la **Supervision** (Monitoring).
6. Appliquez.

Test Final :

- Déconnecte-toi de la console d'admin du Stormshield.
- Logue-toi avec `jsmith` / `password`.
- Essaie de modifier une règle de filtrage -> Tu ne devrais pas pouvoir (grisé ou erreur).
- Va dans les logs ou le dashboard -> Tu devrais voir les infos.