
Lab 7 – Authentication

Table des matières :

1. Création de la politique Lab_7.....	2
2. Mise en place du service LDAP interne.....	3
3. Création manuelle d'un utilisateur John Smith.....	6
4. Enrôlement d'un utilisateur Peter Wood.....	7
5. Tests d'authentification.....	9
6. Filtrage ICMP réservé à John Smith.....	10
7. Redirection des utilisateurs non authentifiés vers le portail captif.....	11
8. Test de la redirection et accès à un site "it".....	12
9. Attribution des droits de supervision à John Smith.....	13
10. Connexion au pare-feu avec le compte John Smith.....	14

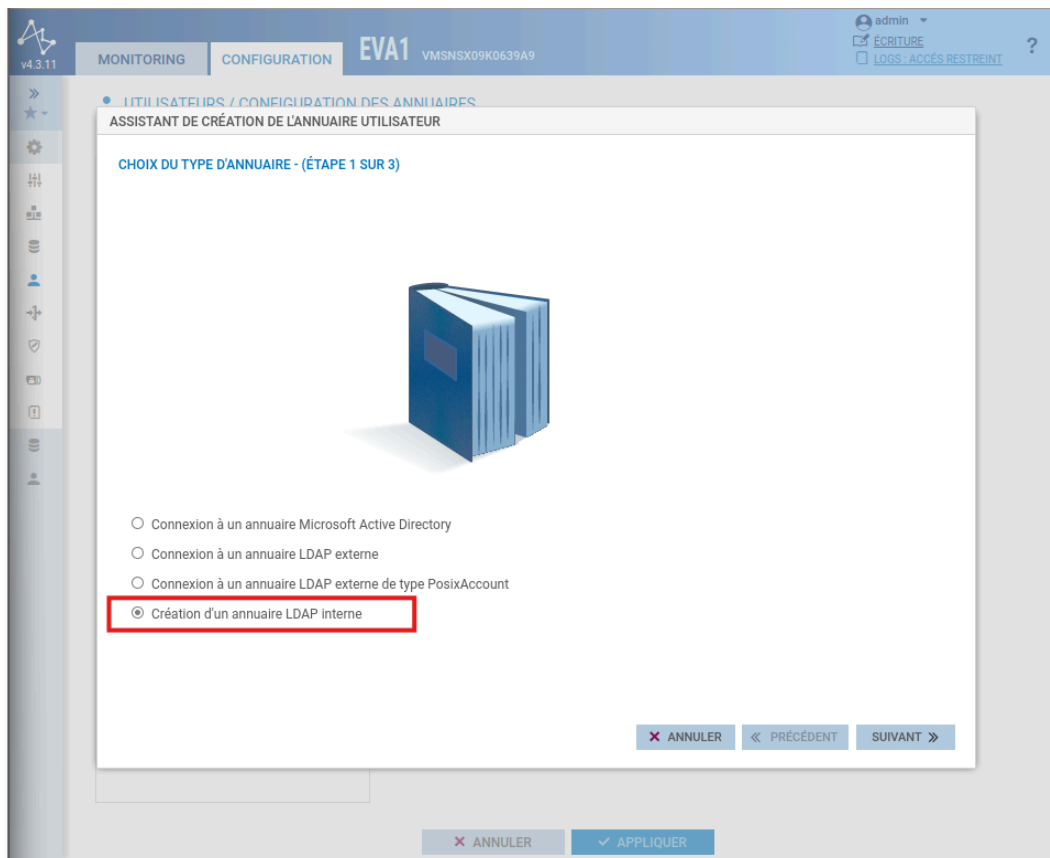
1. Création de la politique Lab_7

- Nous avons commencé par copier la politique de filtrage/NAT « Lab_6 » afin de créer une nouvelle politique baptisée « Lab_7 ». Cette étape permet de reprendre la configuration précédente comme base pour les nouvelles règles liées à l'authentification.

2. Mise en place du service LDAP interne

- À l'aide de l'assistant LDAP, j'ai créé une base LDAP interne avec :
 - Nom de l'organisation : x
 - Domaine : net

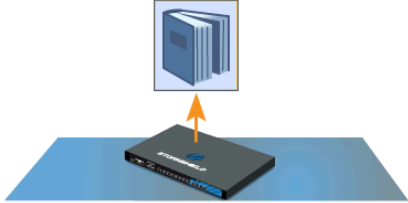
Le profil d'authentification interne a ensuite été activé sur l'interface « IN », avec enrôlement des utilisateurs. Un test d'accès au portail captif via l'adresse <https://192.168.x.254/auth> a permis de valider cette étape.



v4.3.11 MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9 admin ÉCRITURE LOGS - ACCÈS RESTREINT ?

UTILISATEURS / CONFIGURATION DES ANNUAIRES
ASSISTANT DE CRÉATION DE L'ANNUAIRE UTILISATEUR

ACCÈS À L'ANNUAIRE - (ÉTAPE 2 SUR 3)



Organisation: b
Domaine: net
Mot de passe: *****
Confirmer: *****

Excellent

Hachage des mots de passe: SSHA256


ANNULER PRÉCÉDENT SUIVANT

ANNULER APPLIQUER

v4.3.11 MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9 admin ÉCRITURE LOGS - ACCÈS RESTREINT ?

UTILISATEURS / CONFIGURATION DES ANNUAIRES
ASSISTANT DE CRÉATION DE L'ANNUAIRE UTILISATEUR

AUTHENTIFICATION - (ÉTAPE 3 SUR 3)



Activer le profil d'authentification 0 (interne) sur l'interface sélectionnée: in

Activer l'enrôlement des utilisateurs via le profil 0 (interne) du portail Web

Autoriser l'accès à la base LDAP

ANNULER PRÉCÉDENT TERMINER

ANNULER APPLIQUER

← → ↻ Not secure | 192.168.2.254/auth/ ☆ 👤 ⋮

SNSv4

STORMSHIELD
Network Security EN ▾

LOGIN / LOGOUT NEW USER

Username

Authentication duration 4 hours ▾

Logout Login

If you are already authenticated, clicking on connect will extend the authentication by the selected duration

3. Création manuelle d'un utilisateur John Smith

- Un premier utilisateur « John Smith » a été ajouté manuellement avec :
 - Identifiant : jsmith
 - Mot de passe : password
 - Adresse email : jsmith@x.net

The screenshot displays the StormShield user management interface. The top navigation bar includes 'MONITORING' and 'CONFIGURATION' tabs, with 'EVA1' and 'VMSNSX09K0639A9' displayed. The user 'admin' is logged in, with options for 'ÉCRITURE' and 'LOGS - ACCÈS RESTREINT'. The main section is titled 'UTILISATEURS / UTILISATEURS' and contains a search bar, a filter button, and action buttons: '+ Ajouter un utilisateur', '+ Ajouter un groupe', 'X Supprimer', and 'Vérifier l'utilisation'. A list of users is shown with a search bar and a filter button. Below the list, there is a section for creating or modifying a user, with tabs for 'COMPTE', 'CERTIFICAT', and 'MEMBRE DES GROUPES'. The 'COMPTE' tab is active, and the 'Créer ou modifier le mot de passe' button is highlighted. The user details form is filled with: Identifiant (login): jsmith, Nom: smith, Prénom: jonh, E-mail: jsmith@b.net, Téléphone: (empty), and Description: (empty). At the bottom of the form are 'ANNULER' and 'APPLIQUER' buttons.

UTILISATEURS / UTILISATEURS

Rechercher... Filtre + Ajouter un utilisateur + Ajouter un groupe X Supprimer Vérifier l'utilisation

Cn

Utilisez le bouton 'Filtre' pour afficher les utilisateurs et/ou les groupes

Pour créer un utilisateur, renseignez au moins son identifiant et son nom. Pour lui associer un certificat, vous devez aussi indiquer une adresse E-mail valide.

COMPTE CERTIFICAT MEMBRE DES GROUPES

Créer ou modifier le mot de passe

Identifiant (login): jsmith

Nom: smith

Prénom: jonh

E-mail: jsmith@b.net

Téléphone:

Description:

X ANNULER ✓ APPLIQUER

MOT DE PASSE D'AUTHENTIFICATION

Veillez entrer un mot de passe:

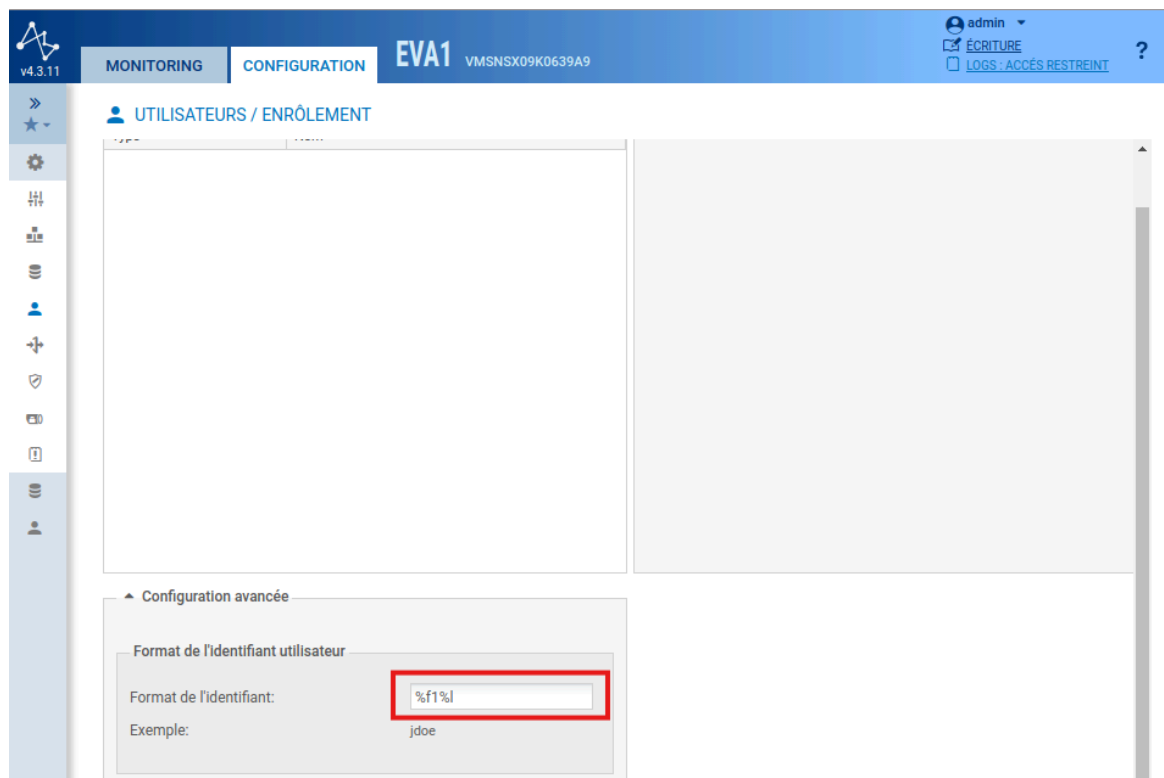
Confirmez le mot de passe:

Faible

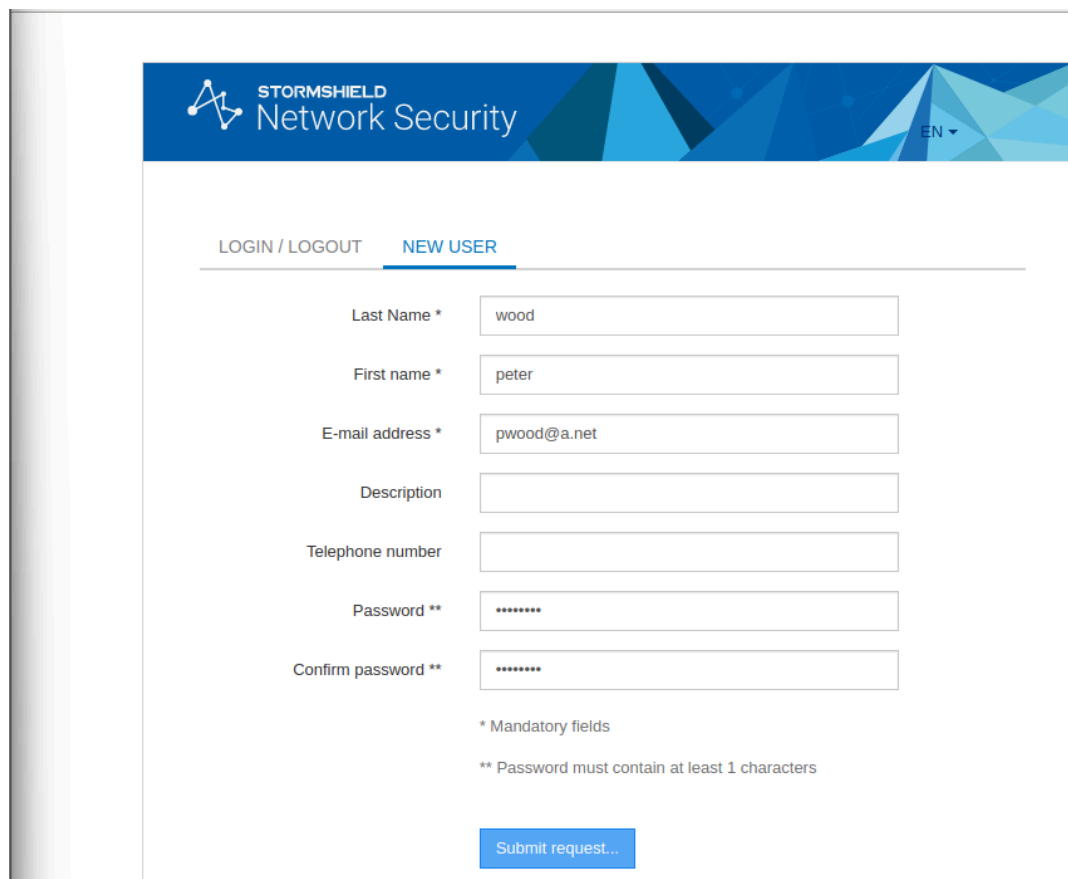
X ANNULER ✓ OK

4. Enrôlement d'un utilisateur Peter Wood

- Ensuite, nous avons utilisé la fonction d'enrôlement pour créer le compte de « Peter Wood » avec le mot de passe password.



The screenshot shows the Stormshield configuration interface. The top navigation bar includes 'MONITORING' and 'CONFIGURATION' tabs, with 'EVA1' and 'VMSNSX09K0639A9' displayed. The user 'admin' is logged in, with options for 'ÉCRITURE' and 'LOGS - ACCÈS RESTREINT'. The main content area is titled 'UTILISATEURS / ENRÔLEMENT'. Below this, there is a section for 'Configuration avancée' with a sub-section 'Format de l'identifiant utilisateur'. The 'Format de l'identifiant:' field is set to '%f1%' and is highlighted with a red box. An example 'jdoe' is shown below.



The screenshot shows the Stormshield Network Security user registration form. The form is titled 'NEW USER' and includes the following fields:

- Last Name *: wood
- First name *: peter
- E-mail address *: pwood@a.net
- Description
- Telephone number
- Password **: *****
- Confirm password **: *****

* Mandatory fields
** Password must contain at least 1 characters

Submit request...

The screenshot displays the STORMSHIELD configuration interface. At the top, the navigation bar includes 'MONITORING' and 'CONFIGURATION' tabs, with 'EVA1' and 'VMSNSX09K0639A9' displayed. The user 'admin' is logged in, with links for 'LECTURE' and 'LOGS - ACCÈS RESTREINT'. The main section is titled 'UTILISATEURS / ENRÔLEMENT'. A table lists users, with 'Utilisateur Peter WOOD' highlighted. A context menu is open over this entry, showing 'Approuver' (checked) and 'Rejeter' options. To the right, a detailed view for 'WOOD' shows fields for 'Identifiant: pwood', 'Nom: WOOD', 'Prénom: Peter', 'Adresse e-mail: pwood@a.net', and 'Description:'.

UTILISATEURS / ENRÔLEMENT

Type	Nom
Utilisateur	Peter WOOD

WOOD

Identifiant: pwood

Nom: WOOD

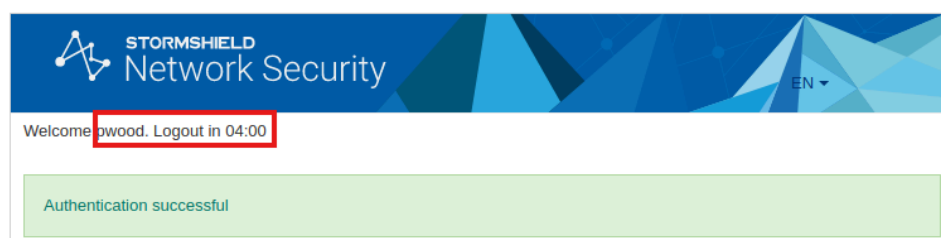
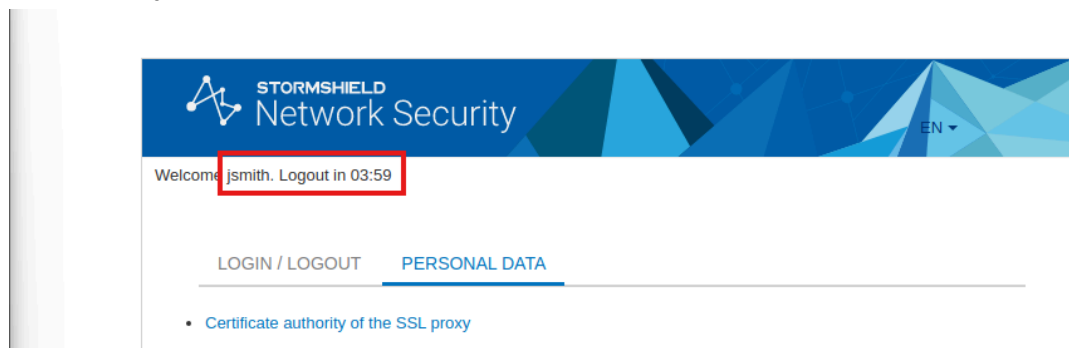
Prénom: Peter

Adresse e-mail: pwood@a.net

Description:

5. Tests d'authentification

- J'ai testé l'authentification de chacun des deux comptes via le portail captif.
 - Les deux comptes ont permis une connexion réussie.
 - Les journaux d'authentification affichent les entrées correspondantes.



6. Filtrage ICMP réservé à John Smith

- Une règle de filtrage a été ajoutée pour que seul l'utilisateur « John Smith » soit autorisé à envoyer des pings (ICMP) depuis le réseau interne.
 - Cette règle génère systématiquement une alarme mineure à chaque utilisation.

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

(7) Lab_7 | Editer | Exporter |

FILTRAGE NAT

Rechercher... | + Nouvelle règle | X Supprimer | ↑ ↓ ↶ ↷ | Couper | Copier | Coller |

	État	Action	Source	Desti...	Port dest.	Protocole	Inspection de sécurité	Com...
FW Administration from Admin PC (contient 1 règles, de 1 à 1)								
internal traffic IN to DMZ (contient 6 règles, de 2 à 7)								
Outgoing traffic (contient 11 règles, de 8 à 18)								
8	on	bloquer	Network_in	Intel geo	http https		IPS	Créée ...
9	on	bloquer	Network_in	www	http https		IPS	Créée ...
10	on	passer	Network_in	Intel	http		IPS Filtrage URL : URLFilter_01	Créée ...
11	on	déchiffrer	Network_in	Intel	https		IPS Filtrage SSL : SSLFilter_0C	Créée ...
12	on	passer	Network_in	Intel	ftp		IPS	Créée ...
13	on	passer	jsmith (Netw	Any	Any	icmp (requête Ech	IPS	Créée ...
14	on	passer	Network_in	Any	Any	icmp (requête Ech	IPS	Créée ...
15	on	passer	Network_in	Intel	ssh		IPS	Créée ...
16	on	passer	srv_dns_priv_A	Intel	dns_udp		IPS	Créée ...
17	on	passer	srv_mail_priv_A	Intel	smtp		IPS	Créée ...
18	on	passer	Network_in	Intel	webmail		IPS	Créée ...
incoming traffic (contient 6 règles, de 19 à 24)								

Page 1 sur 1 | Page courante 1 - 15 sur 15

7. Redirection des utilisateurs non authentifiés vers le portail captif

- Nous avons adapté la politique de filtrage pour que tout utilisateur non authentifié soit redirigé vers le portail captif lors de l'accès à des sites HTTP, à l'exception de ceux appartenant à la catégorie « it ».

The screenshot displays the Stormshield configuration interface for the 'POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT' section. The 'FILTRAGE' tab is active, showing a list of firewall rules. Rule 11 is highlighted with a red border, indicating it is the rule being configured for redirecting unauthenticated users to a captive portal.

État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité	
on	bloquer	Network_in	Internet geo Corée du S	http https	IPS		
on	bloquer	Network_in	www.cnn.com	https http	IPS		
on	passer	j.smith@	Any	Any	icmp (requête Ech	IPS	
on	Portail d'auth Hormis : it	unknown@i	Internet	http	IPS		
on	passer	Network_in	Internet	http	IPS	Filtrage URL : URLFilter_0	
on	déchiffrer	Network_in	Internet	https	IPS	Filtrage SSL : SSLFilter_0C	
on	passer	Network_in	Internet	ftp	IPS		
on	passer	Network_in	Any	Any	icmp (requête Ech	IPS	

8. Test de la redirection et accès à un site "it"

- J'ai testé l'accès à un site classé dans la catégorie « it » pour vérifier qu'il est accessible sans authentification, tandis que les autres sites HTTP déclenchent bien une redirection vers le portail captif.

The image shows two screenshots from a web browser. The top screenshot is a Google search for 'neverssl'. The search results show a link to 'NeverSSL - helping you get online' with the URL 'http://neverssl.com'. Below the search results, there is a notification for 'SNSv4'.

The bottom screenshot shows the Stormshield Network Security login page. The page has a blue header with the Stormshield logo and 'Network Security' text. Below the header, there are links for 'LOGIN / LOGOUT' and 'NEW USER'. The main content area contains a form for authentication with the following fields:


- Username:
- Password:
- Authentication duration:

At the bottom of the form are 'Cancel' and 'OK' buttons. Below the login form, there is a section for 'The NetBSD Project' with a logo, a progress bar showing '\$9,042 raised of \$50,000 goal', and a 'Home' link. The main text for 'The NetBSD Project' states: 'NetBSD is a free, fast, secure, and highly portable Unix-like Open Source operating system. It is available on a wide range of platforms, from large-scale servers and powerful desktop systems to handheld and embedded devices.' There is a '» Learn more' link and a '10.1 available!' announcement.

9. Attribution des droits de supervision à John Smith

- Nous avons ensuite attribué au compte jsmith les droits de supervision sur le pare-feu. Cette étape permet d'autoriser cet utilisateur à accéder aux menus d'administration.

[SYSTÈME / ADMINISTRATEURS](#)

ADMINISTRATEURS		COMPTE ADMIN	GESTION DES TICKETS					
Ajouter un administrateur		Supprimer	↑	↓	Copier les droits	Coller les droits	Donner tous les droits	Passer en vue avancé
	Utilisateur - groupe d'utilisateurs	Système	Réseau	Utilisateurs	Firewall	Supervision	Comptes tempo...	
1	 jsmith@a.net	×	×	×	×	✓	×	

10. Connexion au pare-feu avec le compte John Smith

- Enfin, je me suis connecté à l'interface d'administration du pare-feu avec le compte jsmith afin de valider l'accès aux différents menus. Une authentification sur le portail captif a également été testée avec succès.

