

Activité 7 - Stormshield

Utilisateurs et authentification

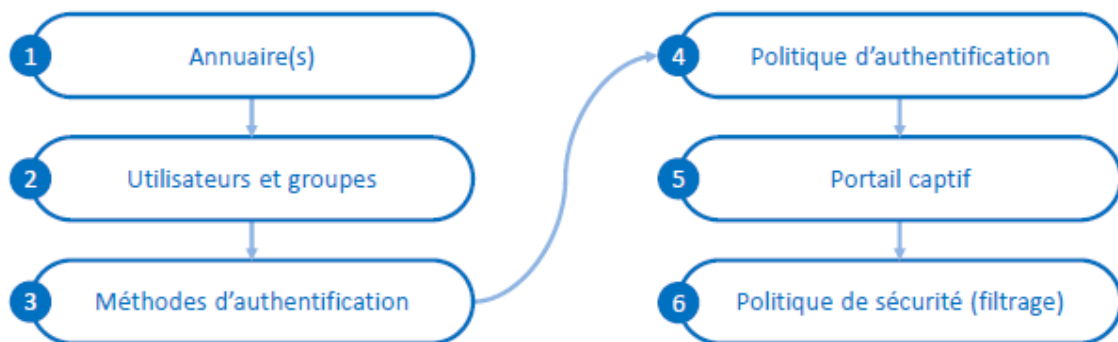
Votre objectif

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 définit 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 configuration sur un firewall consiste à établir un lien vers un ou plusieurs annuaires.

2 - Les utilisateurs sont stockés dans un annuaire et décrits par des attributs (nom, prénom, identifiant, mot de passe, adresse email, 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 - Lightweight Directory Access Protocol

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 si l'assistant de création de l'annuaire ne démarre pas.

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**

ASSISTANT DE CRÉATION DE L'ANNUAIRE UTILISATEUR

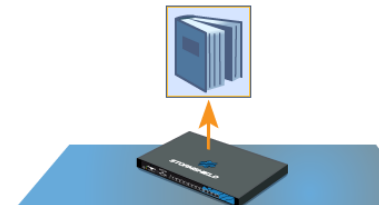
CHOIX DU TYPE D'ANNUAIRE - (ÉTAPE 1 SUR 3)



- ☐ Connexion à un annuaire Microsoft Active Directory
- ☐ Connexion à un annuaire LDAP externe
- ☐ Connexion à un annuaire LDAP externe de type PosixAccount
- ☒ Création d'un annuaire LDAP interne

ASSISTANT DE CRÉATION DE L'ANNUAIRE UTILISATEUR

ACCÈS À L'ANNUAIRE - (ÉTAPE 2 SUR 3)



Organisation: X
Domaine: net
Mot de passe: [masked]
Confirmer: [masked]
Hachage des mots de passe: SSHA256

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 tous les LDAP

5 – Vérifiez que le service est activé

UTILISATEURS / CONFIGURATION DES ANNUAIRES

ANNUAIRES CONFIGURÉS (5 MAXIMUM)

+ Ajouter un annuaire

Domain name

x.net

Configuration

☒ Activer l'utilisation de l'annuaire utilisateur

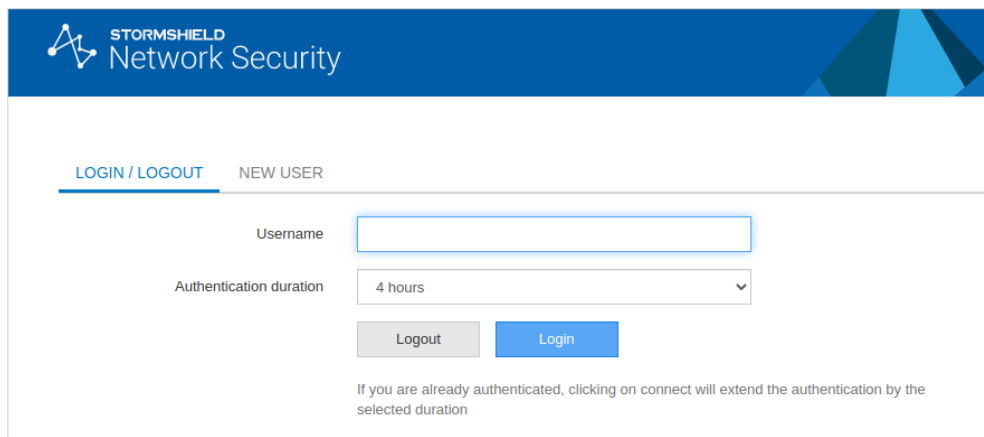
Organisation: x

Domaine: net

Identifiant: cn=NetasqAdmin

Mot de passe:

6 – Testez l'accès au portail captif par <https://192.168.1.254/auth> . La page web suivante doit apparaître.



Gestion des utilisateurs

7 – Créez un utilisateur John Smith :

- Identifiant : **jsmith**
- Nom : **John**
- Prénom : **Smith**
- Adresse email : jsmith@x.net

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



8 – Après 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 des employés de l'entreprise (ce qui doit être le cas) mais certains employés "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'enrôlement".

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%** .

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**



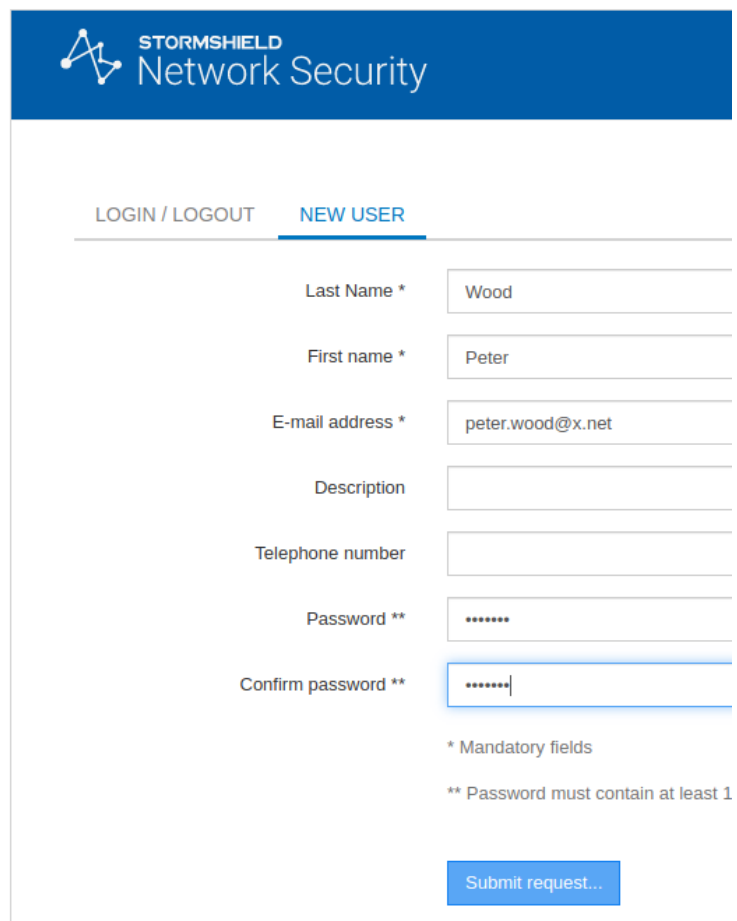
N'oubliez pas de cliquer sur "Appliquer".

👉 10 – Connectez-vous au portail captif <https://192.168.1.254/auth> puis cliquez sur l'onglet **Nouvel Utilisateur**.

Remplissez le formulaire avec les informations nécessaires :

- Utilisateur : **Peter Wood**
- Mot de passe : **mdppeterwood**

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.

UTILISATEURS / ENRÔLEMENT

Rechercher	 Actualiser	Tout sélectionner	 Approuver	 Rejeter
Type	Nom			
Utilisateur	Peter WOOD			

12 – Testez l’authentification de chacun des utilisateurs (John et Peter) depuis le portail captif.
Pour se connecter au portail captif : <https://192.168.1.254/auth>

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.

Pour cela, il faudra ajouter une règle d'authentification avant la règle actuelle pour HTTP, qui contiendra :

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

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

Politique locale (7) Activite_7 [Editer]

FILTRAGE NAT

Rechercher... [Nouvelle règle] [Supprimer]

	État		
			Règle simple
			Séparateur - regroupement de règles
1	on		Règle d'authentification
2	on		Règle d'inspection SSL
			Règle de proxy HTTP explicite
3	on	IN_VERS_DNS	passer
4	on	IN_VERS_WEB	passer

ASSISTANT D'AUTHENTIFICATION



Objectif : Rediriger vers le portail captif les utilisateurs qui ne sont pas authentifiés
Par exemple, lors d'une première authentification ou après expiration de la session.

SOURCE

Qui: les utilisateurs non authentifiés

Depuis: **Network_internals**

DESTINATION

Vers: **Internet**

Hormis pour les URL:

- + Ajouter
- × Supprimer
- authentication_bypass

ANNULER TERMINER

FILTRAGE		NAT							
Rechercher...		+ Nouvelle règle		× Supprimer					
	État	Nom	Action	Source	Destination	Port dest.	Protocole	Inspection	
8	on	Auth_Avant_Internet	Portail d'auth Hormis : authenticat	unknown @ Ne	Internet	http		IPS	

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.

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT									
(6) Filter 06									
FILTRAGE NAT									
Rechercher... + Nouvelle règle ✕ Supprimer ↑ ↓ ↕ ↔ Couper Copier Coller Chercher dans les logs									
		État	Action	Source	Port src.	Destination	Port dest.	Protocole	Inspection de
1		on	passer	srv_dns_priv	Any	Internet	http	DNS	IPS
2		on	Portail d'authentification	unknown @ Net	Any	Internet	http		IPS

- 14 – 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.

SYSTÈME / ADMINISTRATEURS

ADMINISTRATEURS

COMPTE ADMIN

GESTION DES TICKETS

Ajouter un administrateur

✕ Supprimer

↑

↓

Copier les droits

Coller les droits

Donner tous les droits

Utilisateur - groupe d'utilisateurs	Système	Réseau	Utilisateurs	Firewall

SÉLECTIONNER UN UTILISATEUR OU UN GROUPE

☒ Utilisateur - Groupe présent dans l'annuaire LDAP

Utilisateur - Groupe

jsmith@x.net

☐ Utilisateur - Groupe provenant d'un autre domaine (annuaire)

ANNULER

OK

- 15 – 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.

v4.8.14

MONITORING

CONFIGURATION

EVA1

VMSNSX09K0639A9

jsmith@x.net

LECTURE

LOGS : ACCES RESTREINT

LOG / TOUS LES JOURNAUX

Dernière heure

Actualiser

Rechercher...

RECHERCHE DU - 21/05/2026 10:29:41 - AU - 21/05/2026...

DÉTAILS DE LA LIGNE DE LOG

Enregistré à	Action	Utilisateur	Pa
11:29:22	Autoriser		
11:29:22	Autoriser		
11:29:22	Autoriser	Anonymized	

Configuration

Protocole dns_udp

Protocole Internet udp

Règle N° 12

- 16 – BONUS - 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.

Solution :

PASS log:Mineur from jsmith@Network_in to Any Protocol:ICMPMessage: Echo request

ADMINISTRATION DEPUIS PC_admin (contient 2 règles, de 1 à 2)									
1		on	Admin_vers_parefeu	passer	pc_admin	Firewall_in	https		IPS
2		on	ICMP_John_Smith	passer	Any	Any	Any	icmp	IPS