

---

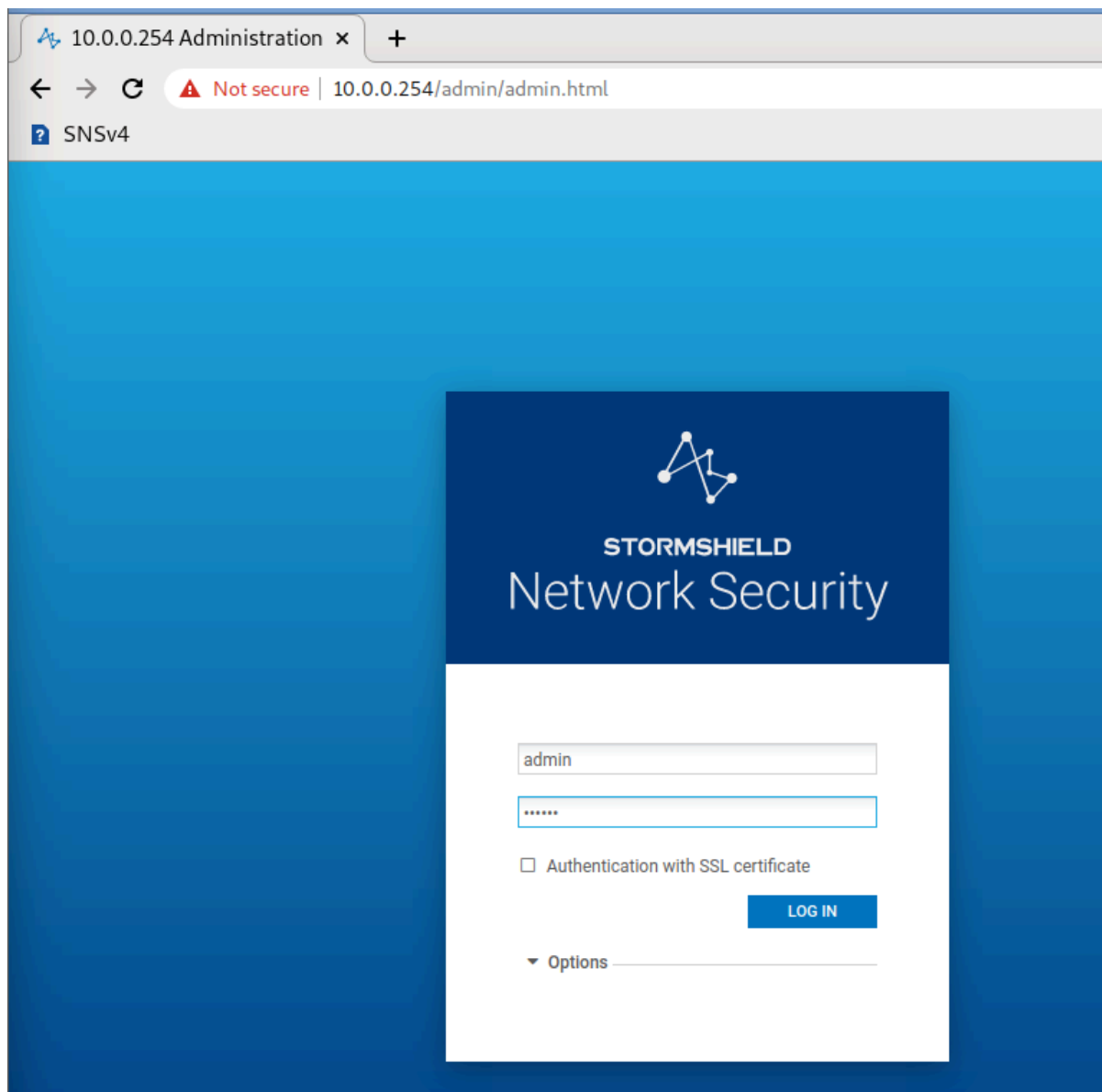
# Lab 1 – Prise en main du Firewall et traces

## Table des matières :

<b>1. Connexion à l'interface d'administration web.....</b>	<b>2</b>
<b>2. Modification des préférences de session.....</b>	<b>3</b>
<b>3. Changement de la langue et du fuseau horaire.....</b>	<b>4</b>
<b>4. Activation du protocole SSH.....</b>	<b>6</b>
<b>5. Vérification de la licence.....</b>	<b>7</b>
<b>6. Changement du mot de passe administrateur.....</b>	<b>8</b>
<b>7. Vérification du stockage local des logs.....</b>	<b>9</b>
<b>8. Sauvegarde de la configuration.....</b>	<b>10</b>

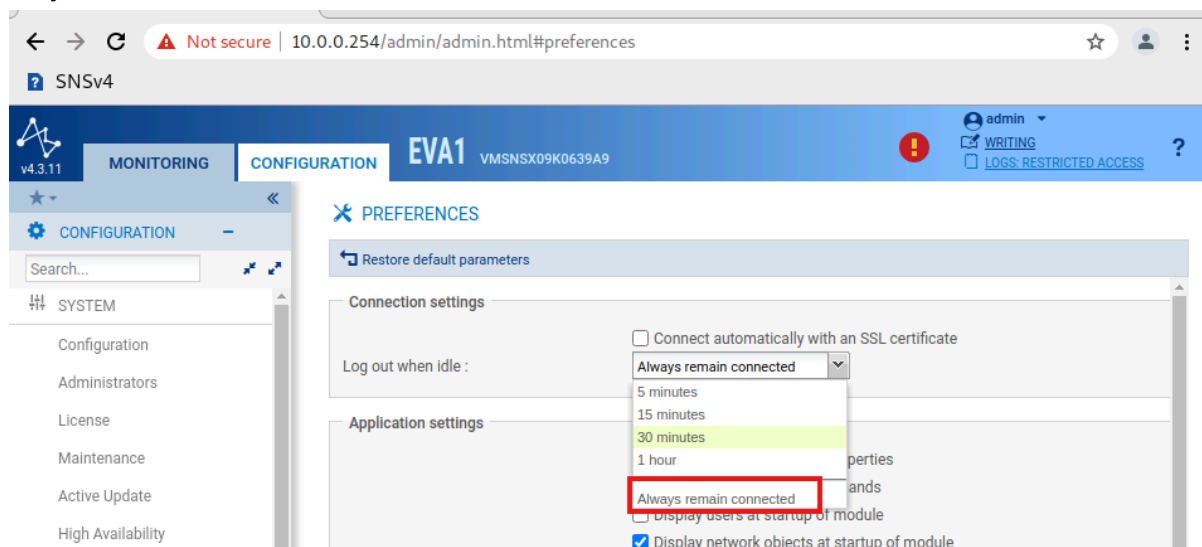
# 1. Connexion à l'interface d'administration web

- Connexion à l'interface d'administration web en y figurant l'utilisateur ainsi que le mot de passe



## 2. Modification des préférences de session

- Nous allons modifier les préférences afin de ne jamais être déconnecté en cas d'inactivité sur l'interface d'administration
- Nous cliquons sur le nom d'utilisateur  Préférences  Déconnexion en cas d'inactivité  Toujours rester connecté



### 3. Changement de la langue et du fuseau horaire

- Pour changer la langue et le fuseau horaire, nous devons aller dans : Système  Configuration

Date/Time settings - 09/08/2025 11:20:20 AM

Manual mode

Synchronize with your machine - 09/08/2025 11:20:22 AM

Synchronize firewall time (NTP)

Time zone:

- ainsi que la langue des messages générés par le firewall dans l'onglet configuration générale :

GENERAL CONFIGURATION   FIREWALL ADMINISTRATION   NETWORK SETTINGS

General configuration

Firewall name:

Firewall language (logs):

Keyboard (console):

- Pour finir nous allons nous reconnecter sur la machine afin de changer la langue :



Identifiant

Mot de passe

S\'authentifier en utilisant un certificat SSL

SE CONNECTER

▲ Options

Français

Lecture seule

## 4. Activation du protocole SSH

- Pour activer le ssh, nous devons aller dans : Système  Configuration  onglet Administration du firewall en cochant Activer l'accès par SSH et Autoriser l'utilisation de mot de passe.

Accès distant par SSH

Activer l'accès par SSH ⓘ

Autoriser l'utilisation de mot de passe

Utiliser le shell nsrpc pour les administrateurs autres que le co

Port d'écoute:

## 5. Vérification de la licence

▪ Nous allons vérifier la validité de notre licence en allant sur : Système  Licence du menu de gauche

Dans les propriétés avancées, nous activons l'installation automatique de la licence.

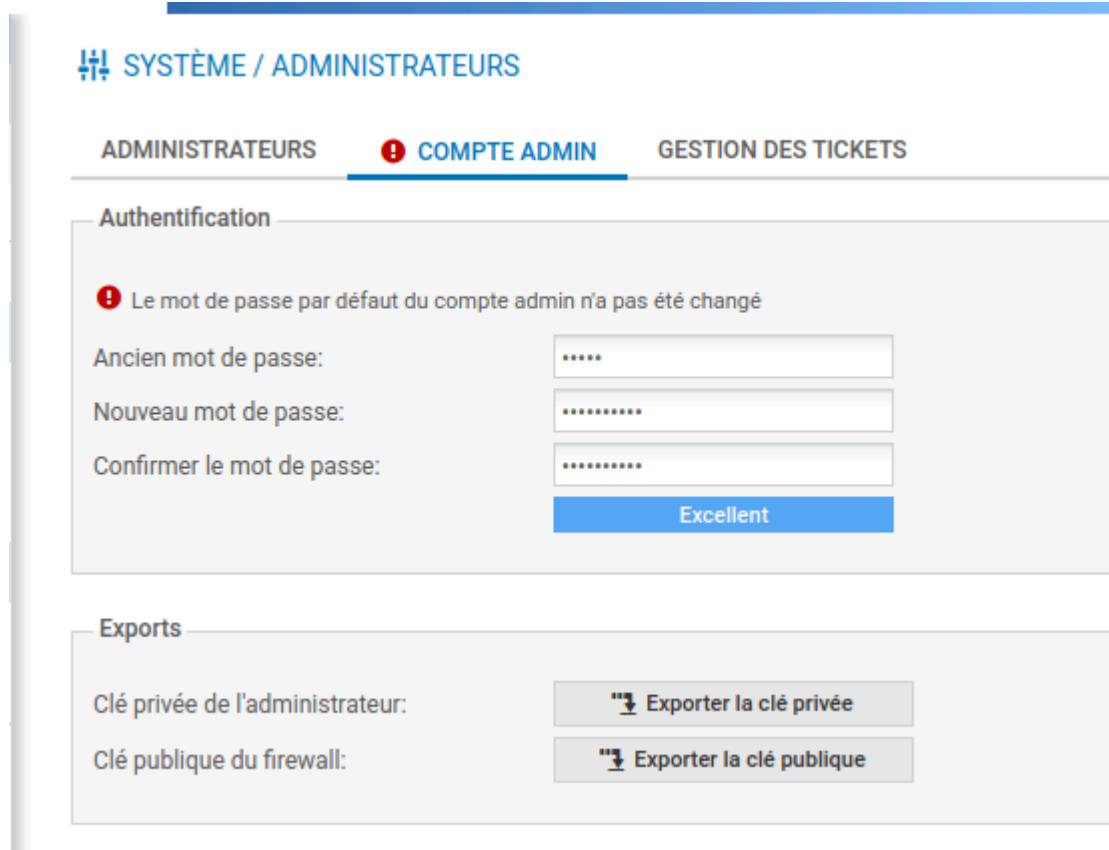
The screenshot shows the 'SYSTÈME / LICENCE' management page. It features two tabs: 'GÉNÉRAL' (selected) and 'DÉTAILS DE LA LICENCE'. Below the tabs, there are two links: 'Rechercher une nouvelle licence' and 'Installer la nouvelle licence'. The main content area displays the following information:

- Date locale sur le Firewall : Lundi 08 Septembre 2025
- Dernière vérification d'une mise à jour de licence effectuée le : Lundi 08 Septembre 2025
- La licence expire dans 4497 jour(s), le Jeudi 31 Décembre 2037.
- La maintenance a expiré depuis 709 jour(s), le Samedi 30 Septembre 2023.
- Management des vulnérabilités a expiré depuis 709 jour(s), le Samedi 30 Septembre 2023.
- Antivirus Avancé a expiré depuis 709 jour(s), le Samedi 30 Septembre 2023.
- L'option Extended Web Control a expiré depuis 709 jour(s), le Samedi 30 Septembre 2023.
- L'option sandboxing Breach Fighter n'a pas été souscrite.
- L'option industrielle a expiré depuis 709 jour(s), le Samedi 30 Septembre 2023.

At the bottom, there is an 'Installer la licence' section with a text input field for the license file and an 'Installer' button.

## 6. Changement du mot de passe administrateur

- La modification du mot de passe se fait dans le menu Système Administrateurs onglet Compte ADMIN.

A screenshot of the Stormshield administration interface. The main heading is 'SYSTÈME / ADMINISTRATEURS'. Below it are three tabs: 'ADMINISTRATEURS', 'COMPTE ADMIN' (which is active and has a red exclamation mark icon), and 'GESTION DES TICKETS'. The 'Authentification' section contains a warning message: 'Le mot de passe par défaut du compte admin n'a pas été changé'. Below this are three password input fields: 'Ancien mot de passe:', 'Nouveau mot de passe:', and 'Confirmer le mot de passe:'. A blue button labeled 'Excellent' is positioned below the confirmation field. The 'Exports' section contains two buttons: 'Exporter la clé privée' and 'Exporter la clé publique', each with a key icon.

## 7. Vérification du stockage local des logs

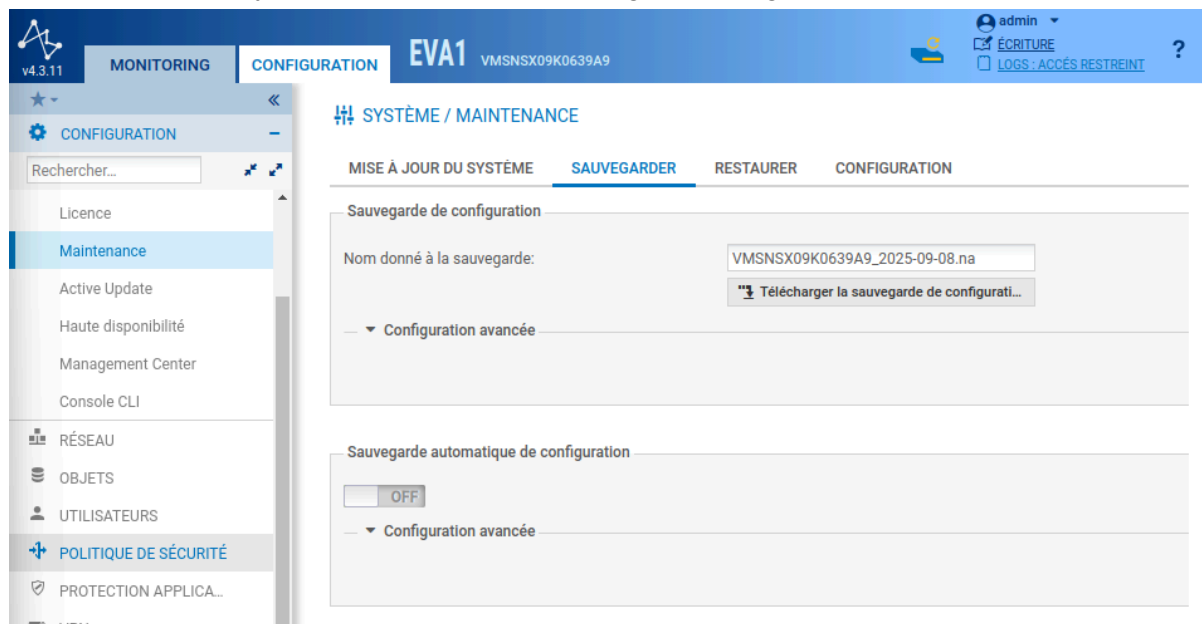
- Nous vérifions que le stockage local des logs est activé dans le disque dur de la VM :  
Configuration  Notifications – Logs – Syslog – IPFIX

The screenshot shows the Stormshield configuration interface. On the left is a navigation menu with categories like SYSTÈME, RÉSEAU, and NOTIFICATIONS. The main area is titled 'NOTIFICATIONS / TRACES - SYSLOG - IPFIX' and has tabs for 'STOCKAGE LOCAL', 'SYSLOG', and 'IPFIX'. The 'STOCKAGE LOCAL' tab is active, showing a toggle switch set to 'ON' and a dropdown menu for 'Périphérique' set to 'Stockage interne 6 Go'. Below this is a table titled 'CONFIGURATION DE L'ESPACE RÉSERVÉ POUR LES TRACES'.

Tout activer		Tout désactiver	
Activé	Famille	Pource...	Quota d'espace disque
<input checked="" type="checkbox"/> Activé	Administration (serverd)	2	122.9 Mo
<input checked="" type="checkbox"/> Activé	Authentification	2	122.9 Mo
<input checked="" type="checkbox"/> Activé	Connexions réseaux	28	1.7 Go
<input checked="" type="checkbox"/> Activé	Evénements systèmes	1	61.4 Mo
<input checked="" type="checkbox"/> Activé	Alarmes	15	921.6 Mo
<input checked="" type="checkbox"/> Activé	Proxy HTTP	10	614.4 Mo
<input checked="" type="checkbox"/> Activé	Connexions applicatives (plugin)	14	860.2 Mo
<input checked="" type="checkbox"/> Activé	Proxy SMTP	4	245.8 Mo
<input checked="" type="checkbox"/> Activé	Politique de filtrage	8	491.5 Mo
<input checked="" type="checkbox"/> Activé	VPN IPsec	2	122.9 Mo
<input checked="" type="checkbox"/> Activé	VPN SSL	2	122.9 Mo
<input type="checkbox"/> Désactivé	Proxy POP3	0	—
<input checked="" type="checkbox"/> Activé	Statistiques	1	61.4 Mo
<input checked="" type="checkbox"/> Activé	Management de vulnérabilités	2	122.9 Mo

## 8. Sauvegarde de la configuration

- Nous réalisons une sauvegarde de la configuration et nous la téléchargeons sur le poste d'administration : Système  Maintenance  onglet Sauvegarder



The screenshot displays the Stormshield configuration interface. The top navigation bar includes 'MONITORING' and 'CONFIGURATION' tabs, with 'EVA1' and 'VMSNSX09K0639A9' displayed. The user is logged in as 'admin' with 'ÉCRITURE' (write) permissions. The left sidebar shows a menu with 'Maintenance' selected. The main content area is titled 'SYSTÈME / MAINTENANCE' and features a sub-menu with 'SAUVEGARDER' (Backup) selected. Under 'Sauvegarde de configuration', the 'Nom donné à la sauvegarde' field contains 'VMSNSX09K0639A9\_2025-09-08.na', and a 'Télécharger la sauvegarde de configurati...' button is visible. The 'Sauvegarde automatique de configuration' section shows a toggle switch set to 'OFF'.