

Activité : Prise en main et configuration initiale

La configuration d'usine par défaut du pare-feu SNS (boîtier ou appliance VM laboratoire) est la suivante :

- la première interface du pare-feu SNS physique est nommée « OUT »,
- la seconde « IN »
- et le reste des interfaces « DMZx ».

L'interface **OUT** est une interface **externe** qui est utilisée pour connecter le pare-feu SNS à **Internet**.

Le reste des interfaces sont **internes** et servent principalement à connecter le pare-feu SNS à des **réseaux locaux** internes.

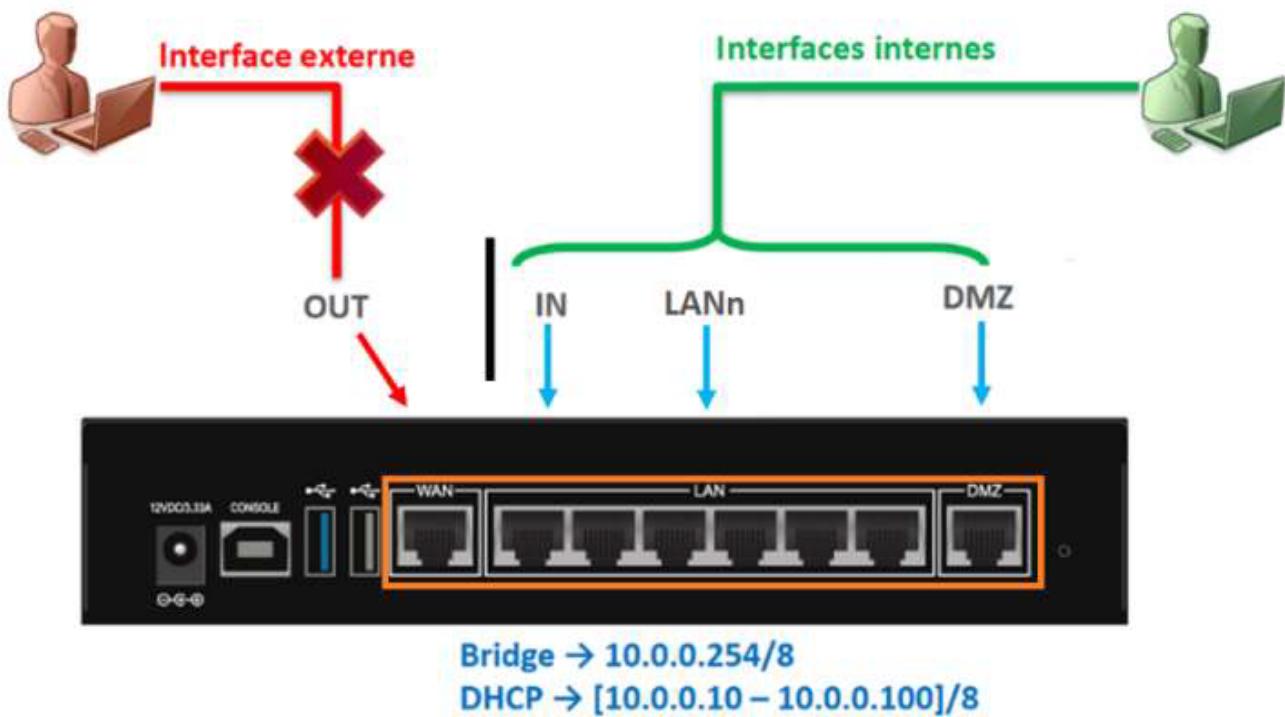
La distinction **interne/externe** pour les interfaces du SNS permet de se protéger contre les attaques d'usurpation d'adresse IP.

Toutes les interfaces sont incluses dans un **bridge** dont l'adresse est **10.0.0.254/8**.

Un **serveur DHCP** est actif sur toutes les interfaces du bridge et il distribue des adresses IP comprises entre **10.0.0.10** et **10.0.0.100**.

L'accès à l'interface web de configuration du pare-feu SNS se fait avec l'url : <https://10.0.0.254>

Par défaut, seul le compte système **admin** (mot de passe par défaut **admin**), disposant de tous les priviléges sur le boîtier, existe et peut se connecter.



Connexion au pare-feu SNS

Pour accéder à l'interface d'administration du pare-feu SNS, il est indispensable de connecter votre client sur une interface interne (IN ou DMZ1) sous peine de devoir redémarrer le firewall qui aura détecté une tentative d'usurpation d'adresse IP sur le bridge et bloquera tout le trafic généré par la machine connectée sur l'interface OUT.

Vérifiez que votre machine hôte a bien obtenu une adresse IP dans la plage 10.0.0.0/24. Le cas échéant utilisez le script de configuration ou configurez-la manuellement.

L'accès à l'interface graphique d'administration du pare-feu SNS se fait par <https://10.0.0.254/admin> à partir d'un navigateur web (de préférence Firefox, Chrome ou Edge). Le compte par défaut est **admin** et le mot de passe **admin**.

Pour des raisons évidentes de sécurité, il conviendra de modifier ce mot de passe lorsque le pare-feu SNS est utilisé en

contexte réel d'entreprise.

Interface d'administration du pare-feu SNS

La page d'accueil de votre pare-feu SNS s'ouvre sur le **Tableau de bord** qui permet de visualiser un certain nombre d'informations sur votre équipement et est personnalisable.

L'INTERFACE D'ADMINISTRATION

The screenshot shows the Stormshield Network Security interface version 4.0.1. The top navigation bar includes the logo, product name, model (EVA1), and serial number (VMSNSX09K0639A9). The top right corner shows the user 'admin' with 'ÉCRITURE / ACCÈS RESTREINT' and a help icon. The main content area is divided into several sections:

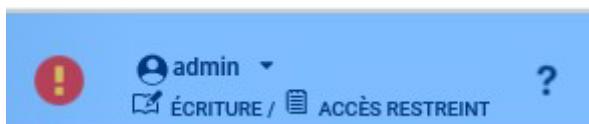
- MONITORING** and **CONFIGURATION** tabs (the latter is highlighted).
- TABLEAU DE BORD** section with a network diagram showing four ports labeled 1, 2, 3, and 4.
- PROPRIÉTÉS** section displaying device details:
 - Nom: VMSNSX09K0639A9
 - Modèle: EVA1
 - Modèle EVA: EVA1
 - Capacité mémoire de l'EVA: 1 Go (1 Go minimum - 2 Go maximum)
 - Nombre de CPU de l'EVA: 1 CPU (1 CPU maximum)
 - Numéro de série: VMSNSX09K0639A9
 - Version: 4.0.1
 - Durée de fonctionnement (uptime): 1h 45m 35s
 - Date: 03/09/2020 16:46:45
 - Date d'expiration de la maintenance: 09/01/2025
- PROTECTIONS** section listing various alerts and events.
- SERVICES** section with icons for Management Center, Active Update, Sandboxing, Cloud Backup, Antivirus, and Reports.
- INDICATEURS DE SANTÉ** section monitoring system health.
- A central box labeled **Contenu du menu** contains a list of menu items.
- A bottom box labeled **Traces de l'interface d'administration** lists recent log entries.
- On the left, a sidebar titled **Menus** lists categories like Rapports, Supervision, and Options.
- At the bottom left, there are buttons for Options, Effacer, and Copier.

L'interface d'administration est découpée en quatre parties :

Partie 1 l'en-tête (partie encadrée en vert)

- contient les informations suivantes :
 - Le **nom** du pare-feu SNS : le nom par défaut est le numéro de série,
 - La **version** du système (firmware),
 - L'**utilisateur connecté** sur l'interface, ses droits d'accès à la configuration : lecture seule

ou écriture et ses droits d'accès aux logs : restreint ou complet,



- Un lien vers **l'aide en ligne** du menu courant ainsi que des informations complémentaires sur les paramètres et les options du menu.
- Cliquez sur la flèche à droite du nom d'utilisateur** (admin) permet d'accéder à plusieurs fonctionnalités :
 - Acquérir ou libérer le droit d'écriture. Notez qu'à un instant donné, un seul utilisateur peut disposer du droit d'écriture sur le pare-feu SNS ;
 - Obtenir le droit d'accès aux données personnelles ;
 - Le menu **Préférences** permet de configurer plusieurs paramètres en relation avec l'interface d'administration. Les plus importants sont :
 - Le **temps d'inactivité** avant de déconnecter l'utilisateur de l'interface d'administration (30 minutes par défaut) ;
 - Les options d'affichage dans les menus (toujours afficher les configurations avancées, nombre de règles de filtrage par page, etc.) ;
 - Liens externes vers les sites Stormshield
 - Se déconnecter** : déconnecte l'utilisateur courant.



Partie 2 Les menus (partie encadrée en rouge)

- Regroupe les menus de configuration, de supervision (Monitoring) ainsi que des raccourcis organisés sous forme de listes rétractables.

Les menus sont séparés en 2 catégories qui s'affichent ensuite sur la zone de menu de gauche constituée d'un ensemble de panneaux qui permettent d'accéder aux différents menus de votre pare-feu SNS.

L'onglet **Monitoring** pour tout ce qui touche à la supervision, les log et l'état du pare-feu SNS.

The screenshot shows a web-based monitoring interface for a network security system. At the top, there's a red-bordered box containing the word "MONITORING". Below it is a navigation bar with a star icon and a back arrow. The main menu includes "TABLEAU DE BORD" and "LOGS - JOURNAUX D'AUDIT", with the latter being the active tab. A search bar labeled "Rechercher..." is also present. The left sidebar lists various log categories: Tous les journaux, Trafic réseau, Alarmes, Web, Vulnérabilités, E-mails, VPN, Évènements système, Filtrage, Analyse sandboxing, and Utilisateurs. At the bottom of the sidebar is a "RAPPORTS" button with a chart icon and a plus sign.

L'onglet **configuration** pour les objets et le paramétrage des diverses fonctionnalités.



Partie 3 Le contenu du menu (partie encadrée en bleu)

- Affiche le contenu du menu sélectionné.

Partie 4 Les traces de l'interface d'administration (partie encadrée en marron)

- Affiche une liste (paramétrable) des logs de l'interface web. On peut y faire apparaître par exemple les commandes NSRPC exécutées par l'interface web, les erreurs levées, les avertissements,

The screenshot shows the Stormshield Network Security System (SNS) dashboard. At the top left, there's a 'TABLEAU DE BORD' button. The main area is divided into several sections:

- RÉSEAU:** Shows four network interfaces labeled 1, 2, 3, and 4.
- PROPRIÉTÉS:** Displays device information:
 - Nom: VMSNSX09K0639A9
 - Modèle: EVA1
 - Modèle EVA: EVA1
 - Capacité mémoire de l'EVA: 1 Go (1 Go minimum - 2 Go maximum)
 - Nombre de CPU de l'EVA: 1 CPU (1 CPU maximum)
 - Numéro de série: VMSNSX09K0639A9
 - Version: 4.0.1
 - Durée de fonctionnement (uptime): 1h 27m 6s
 - Date: 03/09/2020 16:28:16
 - Date d'expiration de la maintenance: 09/01/2025
- SERVICES:** Shows icons for Management Center, Active Update, Sandboxing, Cloud Backup, Antivirus, and Reports.
- PROTECTIONS:** A table listing various protection alerts:

Date	Message	Action	Priorité	Source	Destination
	Active Update: your license has expired (Pvm Data) (1)		1		
	An IP database is unavailable, IP reputation/geolocation disabled. (IPv4) (6)		1		
	An IP database is unavailable, IP reputation/geolocation disabled. (IPv6) (6)		1		
	CPU: Usage exceeded 90% for 10 minutes (1)		1		
	IP address spoofing (type=1) (3)		1		
	Licence: a feature has expired : Sandboxing (1)		1		
	Firewall startup (1)		1		
	Interface up: em0 (1)		1		
	Interface up: em1 (1)		1		
	Interface up: em2 (1)		1		
	Interface up: em3 (1)		1		
- INDICATEURS DE SANTÉ:** Shows icons for various system health metrics: LIEN HA, ALIMENTATION, VENTILATEUR, CPU, MÉMOIRE, DISQUE, RAID, TEMPÉRATURE, and CERTIFICATS.

Le **Tableau de bord**, regroupe l'ensemble des informations et indicateurs du pare-feu SNS :

- État du module Active Update ;
- Alarms ;
- Licence (date d'expiration de chaque module),
- Propriétés (N° de série, politiques actives, date et heure...) ;
- Interfaces (listing des interfaces réseau configurées) ;
- État des différents services.

Un clic sur un élément du tableau de bord renvoie directement vers la page de supervision ou de configuration liée à cet élément.

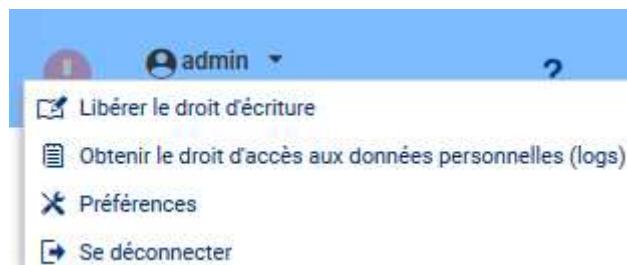
Configuration générale

Voici un certain nombre d'éléments de configuration générale utiles pour la bonne mise en oeuvre de votre pare-feu SNS. Nous étudierons notamment les éléments du menu **Configuration / Système** qui correspond à la configuration générale : licence, mise à jour, mot de passe...

Afin de ne jamais être déconnecté en cas d'inactivité sur l'interface d'administration pendant ces activités pratiques, il conviendra de modifier vos préférences.

En usage réel vous utiliserez un délai de 5 minutes pour éviter de laisser votre session ouverte sur le pare-feu SNS.

- Cliquez sur la flèche à droite de l'icône représentant l'utilisateur connecté en haut à droite.



- Cliquez sur l'icône **Préférences** ;
- Dans la zone **Paramètres de connexion**, sélectionnez dans la liste **Déconnexion en cas d'inactivité** : la valeur **Toujours rester connecté**.

Paramètres de connexion Se connecter automatiquement en utilisant un certificat SSL

Déconnexion en cas d'inactivité :

 Toujours rester connecté **Retour Accueil Stormshield**

- [Stormshield](#)

From:

[/- Les cours du BTS SIO](#)

Permanent link:

</doku.php/reseau/stormshield/phase1?rev=1631480618>Last update: **2021/09/12 23:03**