# 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 privilèges 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

A Network Security	MONITORING CONFIGU	IRATION EVA1 VMSNSX	n-tête		⊖ admin  ▼	
TABLEAU DE BORD	7 TABLEAU DE BORD					
🗐 LOGS - JOURNAUX D'AUDIT 🗕	RÉSEAU			PROTECTIONS	1	
Rechercher				Date Message Action Priorité	Source Destination	
Tous les journaux				🖻 🙀 Active Update: your license has expired (Pvm Data) (1)		
Trafic réseau				🕀 🎾 An IP database is unavailable, IP reputation/geolocation disabled. (IPv4) (6)		
Alarmes				🗉 🁾 An IP database is unavailable, IP reputation/geolocation disab	led. (IPv6) (6)	
Web	PROPRIÉTÉS			T ** ODIN Hanne annual ad 00% for 10 minutes (1)		
web	Nom:	VMSNSX09K0639A9		CPU: Usage exceeded 90% for 10 minutes (1)		
Vulnérabilités	Modèle:	EVA1		IP address spoofing (type=1) (3)		
E-mails	Modèle EVA:	EVA1		Licence: a feature has expired : Sandboxing (1)		
VPN	Capacite memoire de FEVA: 1 Go (1 Go minimum - 2 Go maximum)			E Firewall startup (1)		
Évànamente quetàme	Numéro de série: VMSNSX09K063949			ernewan startup (1)		
Evenements systeme	Version:	4.0.1		Interface up: em0 (1)		
Filtrage	Durée de fonctionnement (uptime):	1h 45m 35s	Contonu	du monu		
Analyse sandboxing	Date:	A 03/09/2020 16:46:45	contenu	uu menu		
Utilisateurs	Date d'expiration de la maintenance	09/01/2025		F Interface up; em3 (1)		
Menus	SERVICES			INDICATEURS DE SANTÉ		
inclus	314	6	6			
	MANAGEMENT CENTER	ACTIVE UPDATE SANDBOXING	CLOUD BACKUP	LIEN HA ALIMENTATION VENTILATEUR CPU	MÉMOIRE DISQUE	
I RAPPORTS +	Ø.	all a				
SUPERVISION +	ANTIVIRUS	RAPPORTS		RAID TEMPÉRATURE CERTIFICATS		
Optio_  II 1525:11 Tableau de bord: MONITOR HEALTH 2314ms						
× Effacer 16:25:12 Tableau de	Trace	Traces de l'interface d'administration				
Copier 16:25:14 Tableau de	ITaces	naces de l'internace d'administration				
III 16:25:14 Tableau de bord: MONITOR SYSTEM 25ms						

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.



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

5/5



### **Retour Accueil Stormshield**

• Stormshield

From: / - Les cours du BTS SIO

Permanent link: /doku.php/reseau/stormshield/phase1?rev=1631480137

Last update: 2021/09/12 22:55

