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				E 🌟 Active Update: your license has expired (Pvm Data) (1)	
Trafic réseau				🗄 🃽 An IP database is unavailable, IP reputation/geolocation disab	led. (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 l'EVA:	1 CPU (1 CPU maximum)		E Firewall startup (1)	
Évànamente quetàme	Numéro de série:	VMSNSX09K0639A9			
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 ▼ III 16:25:11 Tableau de I	bord: MONITOR HEALTH 2314ms				
× Effacer 16:25:12 Tableau de l	bord: MONITOR INTERFACE 185ms	Trace	de l'interf	ace d'administration	
Copier 16:25:14 Tableau de	bord: MONITOR LOG ALARM 24ms	ITaces	suermiteria	ace u autimistration	
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.

5/9



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 apparaitre par exemple les commandes NSRPC exécutées par l'interface web, les erreurs levées, les avertissements,

M TABLEAU DE BORD

RÉSEAU				PROTECTIO	DNS				
		100		Date	Message	Action	Priorité 1	Source	Destination
	123	4		🗄 🌋 Active	Update: your license has	expired (Pvm Da	sta) (1)		
				🗄 🌋 An IP o	database is unavailable, l	P reputation/geo	location disable	ed. (IPv4) (6)	
ρρορριέτές				🗄 🎬 🗥 IP a	database is unavailable, l	P reputation/geo	location disable	ed. (IPv6) (6)	
PROPRIETES	VMCNEY00K0620A0			🕀 管 CPU: U	Jsage exceeded 90% for	10 minutes (1)			
Modèle:	FVA1			E 👘 ID and a		6			
Modèle EVA:	EVA1				rress spooning (type=1) (3	9			
Capacité mémoire de l'EVA:	1 Go (1 Go minimum - 2	Go maximum) 0		E 📽 Licenc	e: a feature has expired :	Sandboxing (1)			
Nombre de CPU de l'EVA:	1 CPU (1 CPU maximum) 🕚			artup (1)				
Numéro de série:	VMSNSX09K0639A9			⊕ Interface u	ip: em0 (1)				
Version:	4.0.1								
Durée de fonctionnement (uptime):	1h 27m 6s			t Interface u	ip: em1 (1)				
Date:	03/09/2020 16:28:16			⊕ Interface u	ıp: em2 (1)				
Date d'expiration de la maintenance	e: 09/01/2025			⊞ Interface u	ıp: em3 (1)				
SERVICES				INDICATEU	RS DE SANTÉ				
	0.	6	۵	9	₩.	×			
MANAGEMENT CENTER	ACTIVE UPDATE	SANDBOXING	CLOUD BACKUP	LIEN HA	ALIMENTATION	VENTILATEUR	CPU	MÉMOIRE	DISQUE
Ø,					R≡	0.			
ANTIVIRUS	RAPPORTS			RAID	TEMPÉRATURE	CERTIFICATS			

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

- État du module Active Update ;
- Alarmes ;
- 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.

2025/08/15 11:32	7/9	Fiche savoirs technologiques : Prise en main et configuration initial	e du SNS
Paramètres de con	nexion		
		Se connecter automatiquement en utilisant un certificat SSL	

Toujours rester connecté

- Sélectionnez dans le menu à gauche Configuration / Système puis Configuration. Le volet Configuration générale est affiché.
- Commencez par donner un nom à votre boîtier : FWX AgenceX et changer la langue de la console. Laissez les logs en anglais.

CONFIGURATION GÉNÉRALE	ADMINISTRATION DU FIREWALL	PARAMÈTRES RÉSEAUX
Configuration générale		
Nom du firewall:	FWA_Agence/	Ą
Langue du Firewall (traces):	Anglais	-
Clavier (console):	Français	

 La zone Politique de mots de passe permet de définir la longueur du mot de passe (8 par défaut) et la zone Types de caractères obligatoires permet de gérer la complexité du mot de passe (Aucun, Alphanumériques, alphabétiques et spéciaux).

Politique de mots de passe		
Longueur minimale des mots de passe :	8	~
Types de caractères obligatoires :	Aucun	~

• Modifiez le fuseau horaire dans la zone Date et heure (Europe/Paris).

Déconnexion en cas d'inactivité :

- Cliquez Synchroniser avec votre machine ou Maintenir le firewall à l'heure (NTP) pour que les mises à jour d'heure d'été/heure d'hiver soient également effectives.
- Cliquez le bouton Appliquer pour sauvegarder la configuration et Redémarrer plus tard.

Voici quelques commandes rapides pour réaliser le paramétrage initial du pare-feu SNS.

- La modification du mot de passe admin (recommandée) se fait dans le menu Configuration / Système / Administrateurs onglet Compte ADMIN. Le mot de passe doit par défaut, comporter au moins 5 caractères. La force du mot de passe choisit s'affiche alors. Les boutons Exporter la clé privée et Exporter la clé publique du firewall permettent respectivement de télécharger la clé privée et clé publique du compte admin.
- La sauvegarde de la configuration se fait dans le menu Configuration / Système / Maintenance onglet Sauvegarder. La sauvegarde automatique du fichier de configuration peut être mise en place et effectuée sur le Cloud Stormshield.
- L'accès SSH s'active depuis le menu Configuration / Système / Configuration onglet Administration du firewall, cochez Activer l'accès par SSH et Autoriser l'utilisation de mot de passe, puis choisissez ssh dans Port d'écoute.

Accès distant par SSH	
	📧 Activer l'accès par SSH 🤨
	Autoriser l'utilisation de mot de passe
Port d'écoute:	ssh 🛛 🗙 💌

- Le menu Configuration / Système / Maintenance onglet Mise à jour du système permet de mettre à jour le système le cas échéant. Afin d'appliquer un fichier de mise à jour firmware, vous devrez le télécharger sur l'UTM (soit directement via le lien Rechercher de nouvelles mises à jour, soit en allant le télécharger sur le site https://mystormshield.eu). Nous allons procéder à la mise à jour vers la dernière version disponible que vous aurez au préalable téléchargée.
- Cliquez Configuration / Système / Maintenance onglet Mise à jour du système.

MISE À JOUR DU SYSTÈME	SAUVEGARDER	RESTAURER	CONFIGURATION	
Mises à jour disponibles				
Aucune mise à jour disponible				
Q Rechercher de nouvelles mis	es à jour			
Mise à jour du système				
Sélectionnez la mise à jour:		C:\fakepath\	fwupd-4.0.3-SNS-amd64-XL-VM.maj	444.5

	C Mettre à jour le firewall
 Configuration avancée 	
Action:	Télécharger le firmware et l'activer
	O Télécharger le firmware
	O Activer le firmware précédemment téléchargé
/ersion actuelle du système:	4.0.1
Mise à jour présente sur le firewall:	Aucune mise à jour n'est présente sur le firewall

- Sélectionnez le fichier de mise à jour présent sur votre poste de travail.
- Dépliez la zone Configuration avancée.
- Dans la configuration avancée, vous pouvez choisir de Télécharger le firmware et l'activer ce qui appliquera la mise à jour ou bien de la télécharger uniquement, son activation pourra se faire ultérieurement avec l'option Activer le firmware précédemment téléchargé.
- Dans la zone Configuration avancée choisir Télécharger le firmware et l'activer
- Cliquez le bouton Metre à jour le firewall.

L'opération prendra plusieurs minutes surtout ne débranchez pas le pare-feu pendant la mise à jour. Le pare-feu sera ensuite redémarré.

Reconnexion automatique sur 10.0.0.254

Le boitier est en cours de mise à jour. Cela peut prendre plusieurs minutes. L'application se reconnectera automatiquement. Ne débranchez pas votre firewall durant cette opération.

Temps restant estimé : 19s

* Le menu **Configuration / Système / Maintenance** onglet **Configuration** permet uniquement sur les boitiers physiques de déterminer la partition active et ainsi de garder deux versions du système disponibles avec une partition de sauvegarde qui permet de revenir en arrière sur le boitier (firmware n-1, config n-1).

NB : Pour revenir à une configuration ou version n-2 ou supérieure il faut utiliser USB Recovery.

* Le menu **Configuration / Système / Active update** permet de contrôler la mise à jour automatique des modules de Bases d'URLs embarquées, IPS : Signatures de protection contextuelles, Géolocalisation / Réputation IP publiques, signatures antispam, antivirus et autres listes noires préconfigurées par Stormshield. Vous pouvez le cas échéant les désactiver mais au contraire vérifiez qu'elles sont bien toutes activées. * Le menu **Configuration / Système / Licence** affiche les détails de la licence et permet le cas échéant de l'installer (à récupérer par l'administrateur sur le site mystormshield.eu avec les informations figurant sous le boitier). À noter que si vous n'activez pas la licence au bout d'un certain temps les fonctionnalités se réduisent et surtout vous ne pourrez pas stocker les logs sur les boitiers physiques.

==== Stockage des logs : onglet Configuration / Notifications / Traces - Syslog - IPFIX ==== * L'activation du stockage local des logs s'effectue dans l'onglet Configuration / Notifications / Traces - Syslog - IPFIX / Stockage local * Sur une machine virtuelle, celui-ci est activé par défaut et occupe un espace disque de 6Go.

NOTIFICATIONS / TRACES - SYSLOG - IPFIX

STOCKAGE LOCAL	SYSLOG	IPFIX		
DN				
Support de stockage				
212 A C C C C		122 1 22 220	O • • •	

