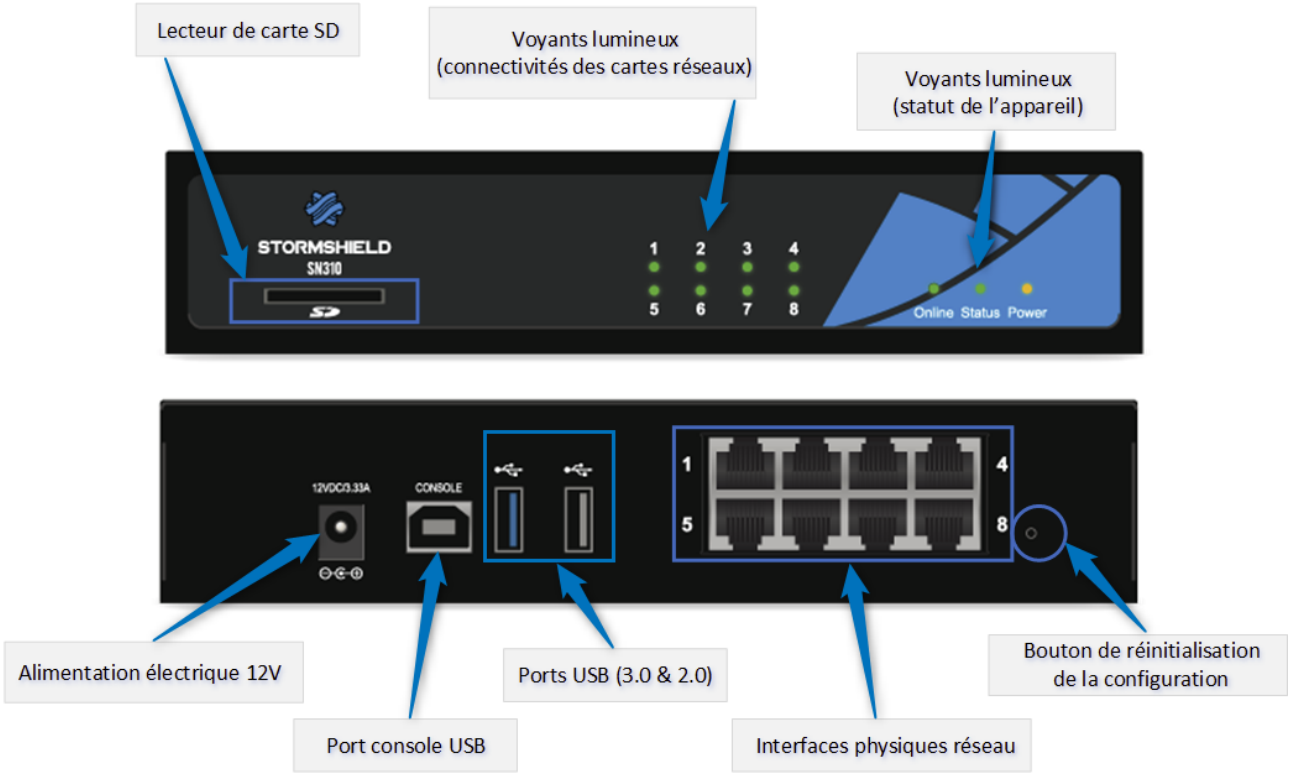
Documentation : Configuration complète du Pare-feu Stormshield SN510

Ce document présente les étapes essentielles et avancées pour l'installation, la configuration initiale, la sécurisation et la gestion du pare-feu Stormshield SN510. Il contient des illustrations pour guider l'administrateur réseau dans la prise en main de l'interface.

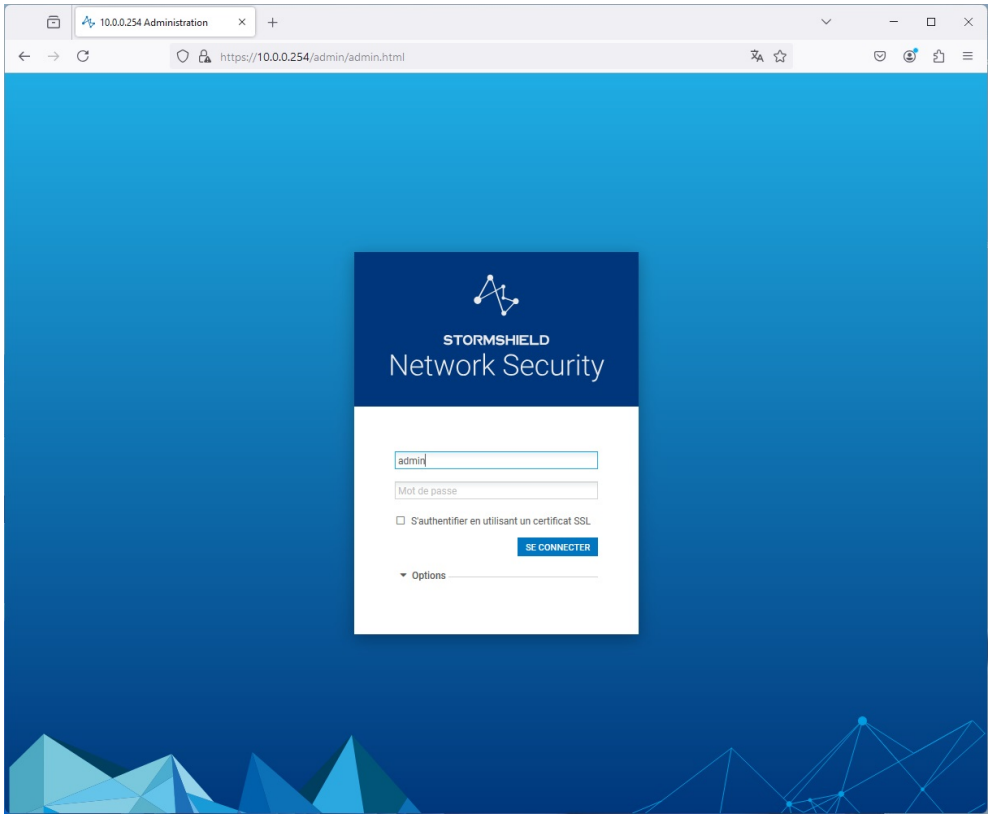
1. Présentation matérielle du SN510

Le SN510 offre plusieurs ports réseau RJ45, deux ports USB (2.0 et 3.0), une console USB pour le débogage, un port d'alimentation 12V et un bouton de réinitialisation. L'image suivante illustre ces composants physiques.



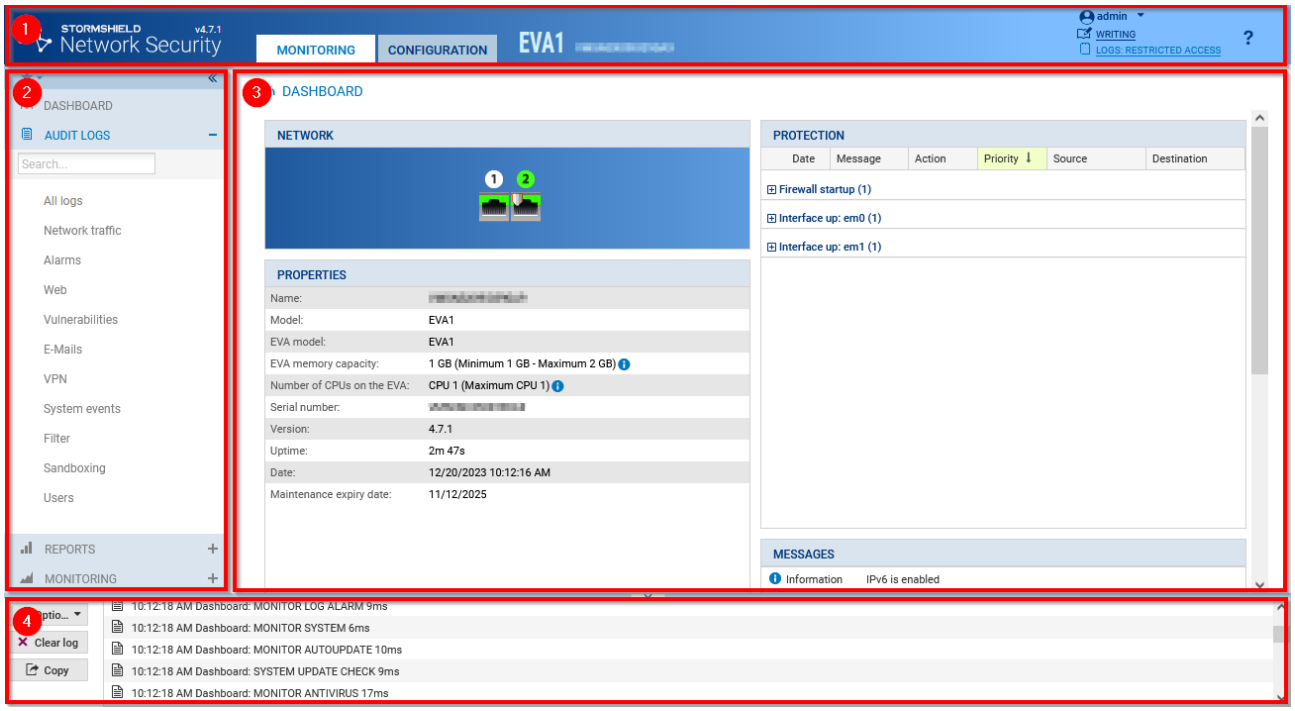
2. Connexion à l'interface Web

Branchez un câble réseau sur une interface LAN et accédez à l'interface via un navigateur avec l'adresse https://192.168.1.1. Connectez-vous avec l'identifiant 'admin' et le mot de passe par défaut. Vous serez ensuite invité à changer ce mot de passe.



3. Découverte de l'interface d'administration

L'interface se compose de plusieurs parties : un tableau de bord central, une barre de menus à gauche pour naviguer dans les journaux, le trafic, les VPN, etc. L'en-tête donne accès aux paramètres d'utilisateur et de configuration générale.

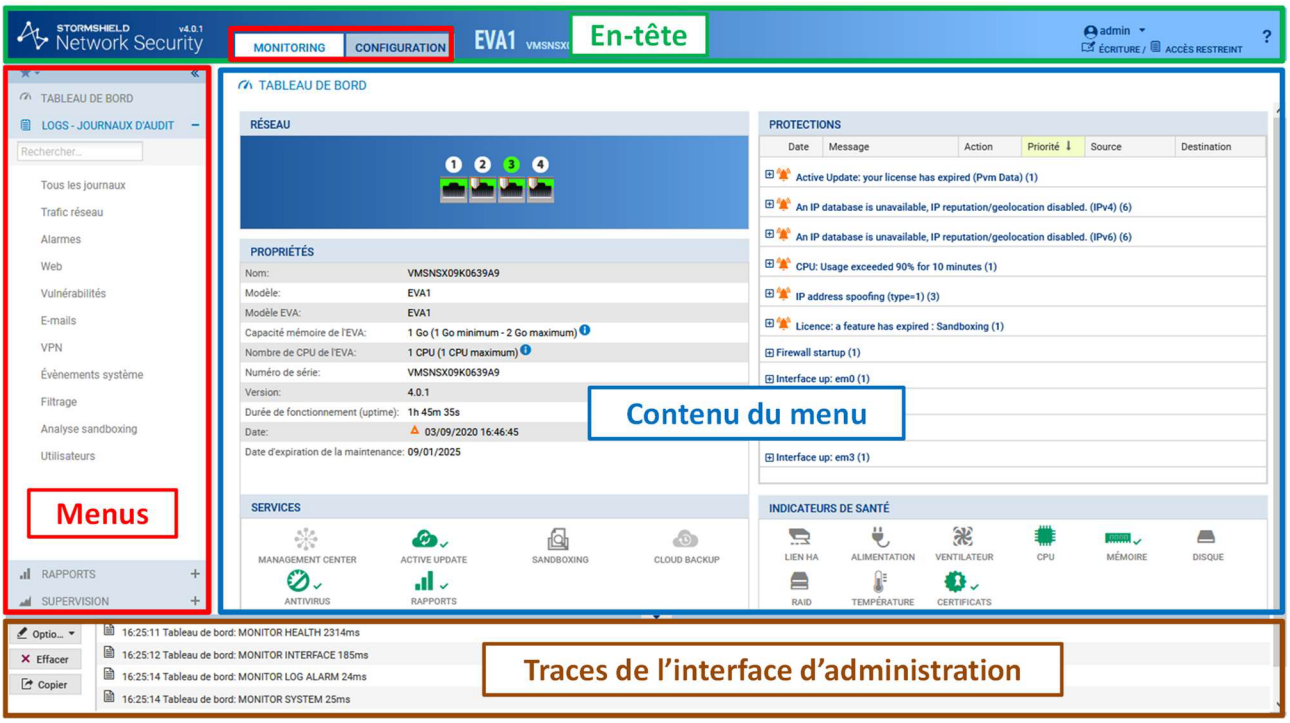


4. Tableau de bord et informations système

Le tableau de bord fournit des informations en temps réel : état des interfaces réseau, alertes de sécurité, usage CPU/mémoire, date de mise à jour, etc. Ces indicateurs permettent une surveillance

rapide de l'état de santé du pare-feu.

L'INTERFACE D'ADMINISTRATION



5. Configuration des interfaces réseau

Dans l'onglet 'Configuration > Réseau', attribuez des adresses IP aux interfaces selon votre plan d'adressage. Vous pouvez définir des zones (LAN, WAN, DMZ) et appliquer des politiques de sécurité spécifiques à chacune.

6. Politiques de filtrage et NAT

Les politiques de sécurité permettent d'autoriser ou bloquer le trafic entre zones. Utilisez l'onglet 'Filtrage' pour définir des règles en fonction des adresses IP, protocoles, ports, horaires, etc. Ajoutez une règle NAT pour l'accès Internet.

7. Configuration VPN

Stormshield prend en charge IPsec et SSL VPN. Pour une connexion site-à-site, configurez les deux extrémités avec des paramètres identiques (algorithmes, clé pré-partagée). Pour l'accès distant, utilisez le client SSL Stormshield, ajoutez les utilisateurs et configurez l'accès.

8. Gestion des utilisateurs et authentification

Ajoutez des utilisateurs locaux ou connectez-vous à un annuaire LDAP. Activez l'authentification par portail captif si nécessaire. Vous pouvez associer les utilisateurs à des groupes avec des droits

spécifiques.

9. Sauvegarde et mises à jour

Effectuez une sauvegarde manuelle ou automatique de la configuration via l'interface. Téléchargez les dernières mises à jour depuis le site Stormshield ou configurez une mise à jour automatique avec accès Internet.

10. Bonnes pratiques de sécurité (recommandations ANSSI)

- Désactivez les services inutiles.

- Changez les mots de passe par défaut et activez 2FA.

- Limitez l'accès d'administration à une liste blanche d'IP.

- Appliquez régulièrement les correctifs de sécurité.