PROCEDURE D'INSTALLATION : CONFIGURATION

PROJET

CUB

- **Objectif :** Assurer la sécurité du réseau via le filtrage du trafic, le chiffrement des communications (VPN), la gestion sécurisée, la surveillance des événements et la sauvegarde des configurations, afin de garantir la confidentialité, l'intégrité et la disponibilité des systèmes.

- **Prérequis**

  - **Système d’exploitation**
    - OS Stormshield

  - **Ressources matérielles (minimum recommandé)**
    - **CPU** : 1 cœurs
    - **RAM** : 1 Go
    - **Disque** : 32 Go (SSD recommandé)
    - **Connexion réseau** : 1 Gbit/s

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.

Interface de pare-feu SNS

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

1. **L’en-tête (partie encadrée en vert) :** Elle contient les informations suivantes :
   - Le nom du firewall : 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 du menu courant ainsi que des informations complémentaires sur les paramètres et les options du menu. Notez que les pages d’aide ne sont pas embarquées mais redirigent vers Internet.

   Cliquer sur le nom d’utilisateur permet d’accéder à plusieurs fonctionnalités :
   - 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.
     - Acquérir ou libérer les droits d’écriture. Notez qu’à un instant donné, un seul utilisateur peut disposer du droit d’écriture sur le firewall.
     - Accéder aux données personnelles.
     - Déconnecter l’utilisateur.

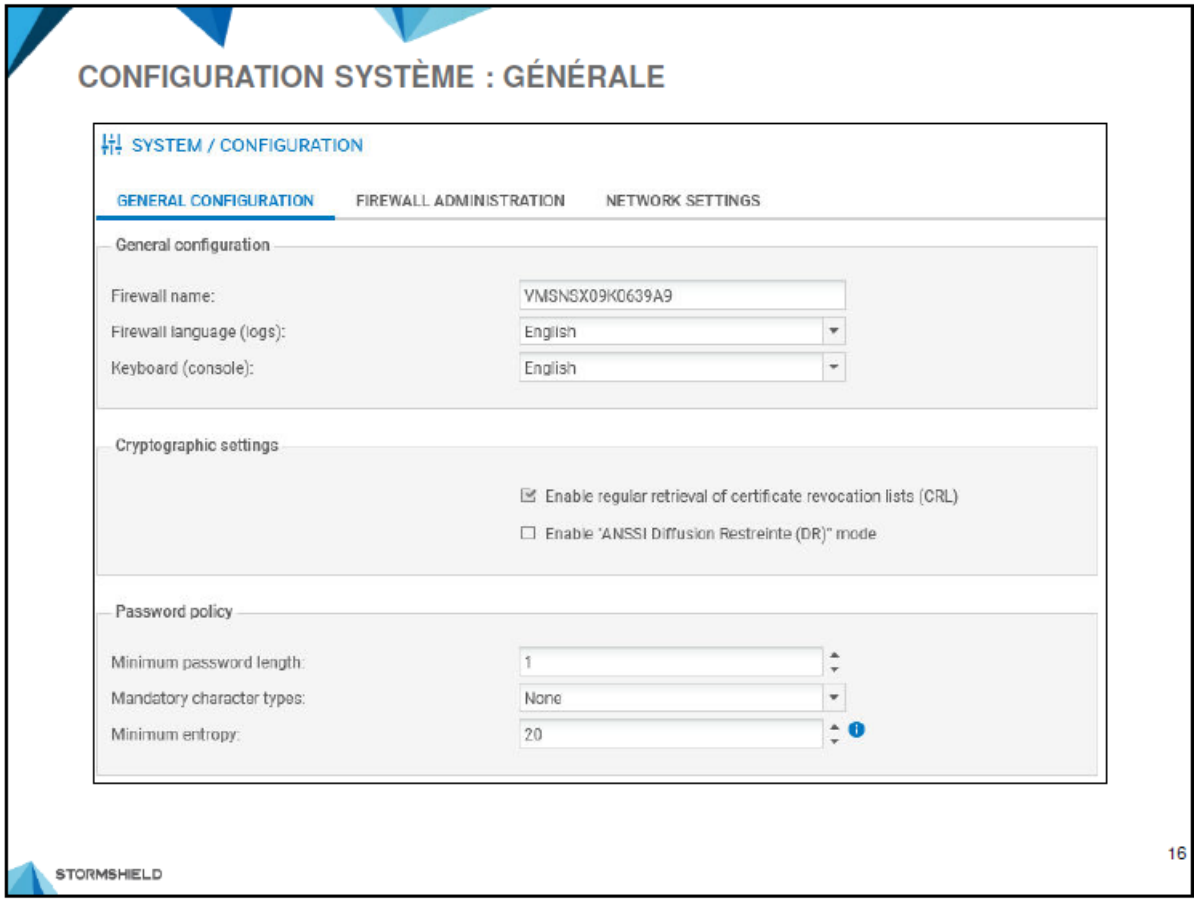
2. **Les menus (partie encadrée en rouge) :** Regroupe les menus de configuration, de supervision ainsi que des raccourcis organisés sous forme de listes rétractables. Les menus sont séparés en 2 catégories. L’onglet supervision pour tout ce qui touche à la supervision, les log et l’état du firewall. L’onglet configuration pour les objets et le paramétrage des diverses fonctionnalités.

3. **Le contenu du menu (partie encadrée en bleu) :** Affiche le contenu du menu sélectionné.

4. **Les logs de la webUI (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, ….

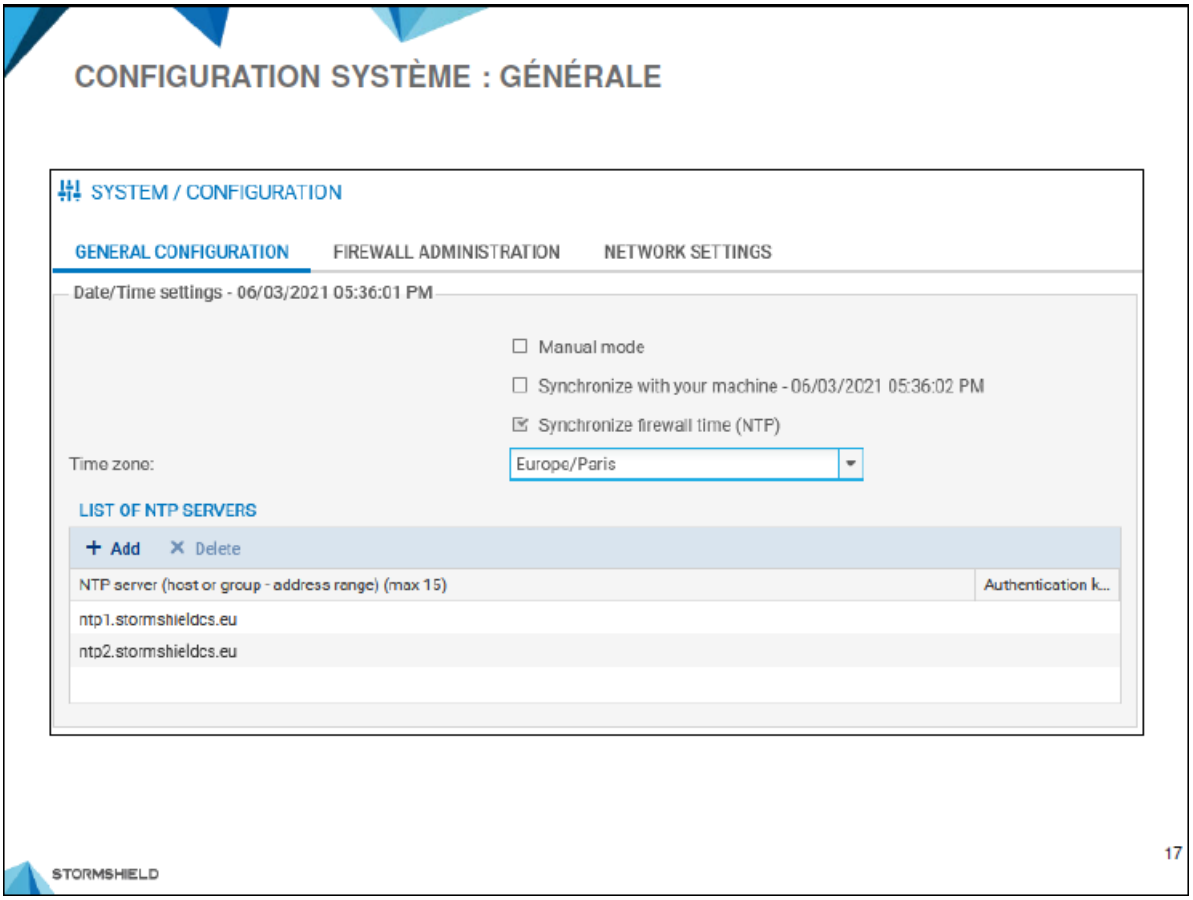
Configuration du système



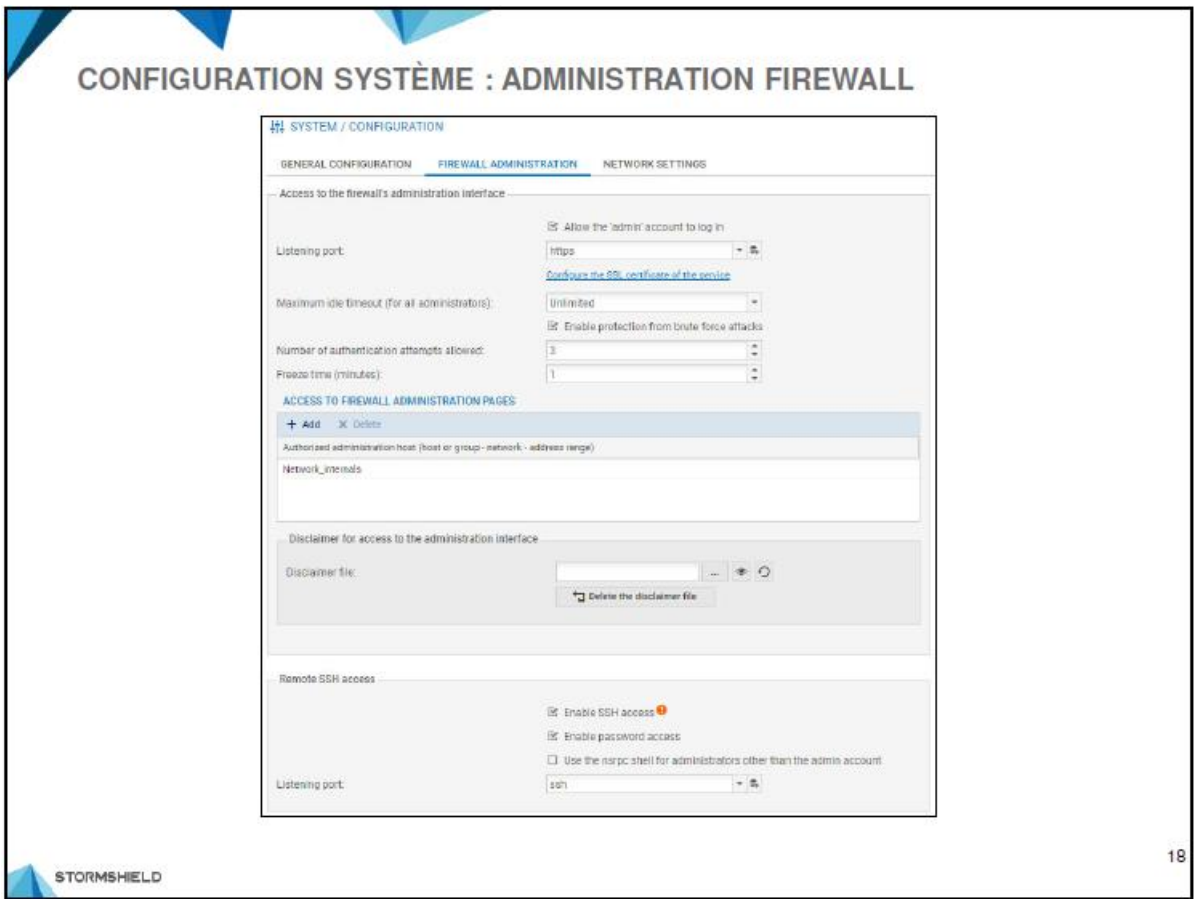
Le menu CONFIGURATION ⇒ SYSTÈME ⇒ Configuration permet de configurer les paramètres systèmes, administratifs et réseaux du firewall. Il est composé de trois onglets :

1. **CONFIGURATION GÉNÉRALE :**

- Le nom du firewall qui par défaut est le numéro de série.
- La langue des traces remontées par le firewall (Anglais ou Français).
- La disposition du clavier utilisée pour un accès console direct (Anglais, Français, Italien, Polonais ou Suisse).
- Les paramètres cryptographiques regroupent deux options qui sont respectivement en relation avec les certificats (présentés dans la formation Expert) et le mode « ANSSI Diffusion Restreinte (DR) ».
- La politique de mots de passe fixe la longueur minimale et les caractères requis pour les mots de passe du firewall (utilisateurs LDAP, sauvegardes, certificats). Par défaut, un seul caractère est requis, mais l'administrateur peut imposer des mots de passe alphanumériques ou avec caractères spéciaux et ajuster la longueur minimale.



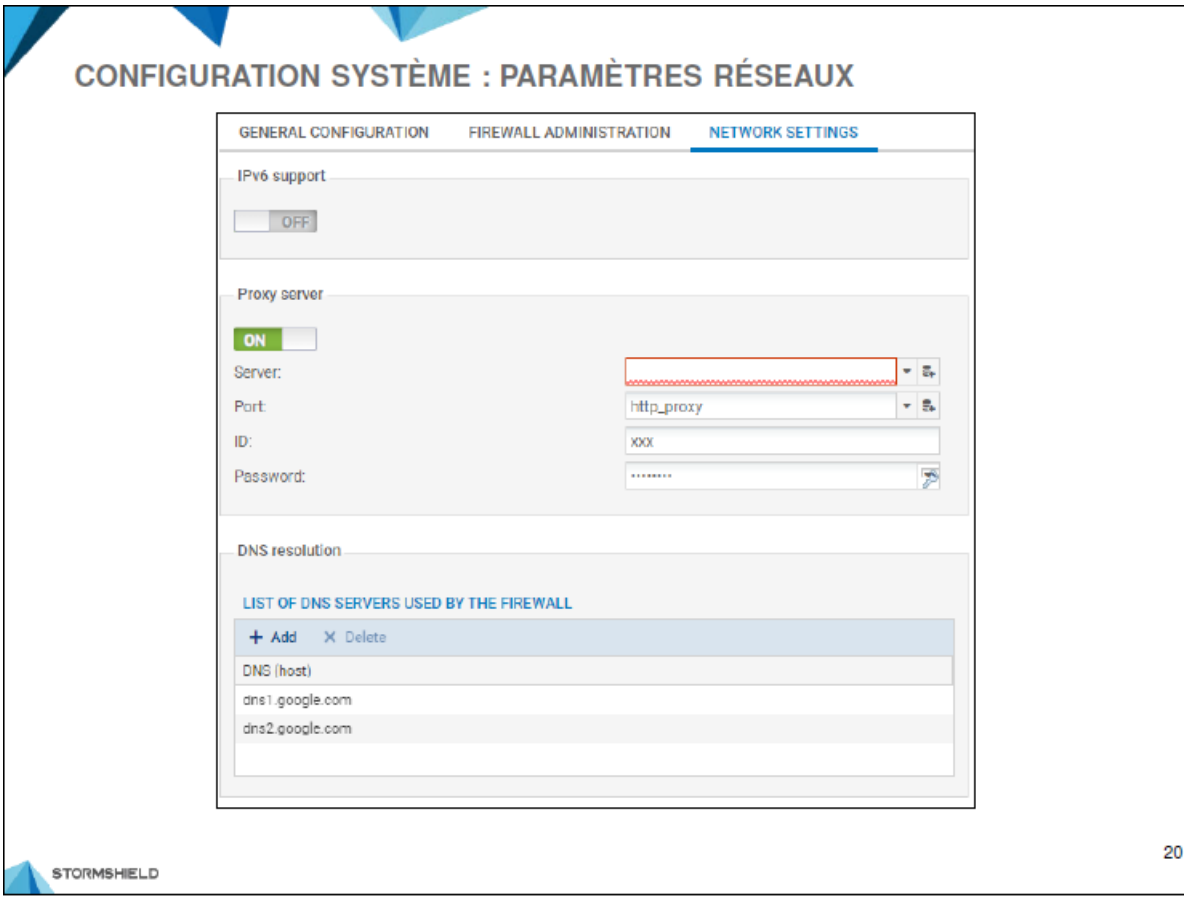
- Les paramètres horaires : date, heure et fuseau horaire. Ces paramètres sont cruciaux pour des fonctionnalités telles que les logs ou l'authentification. La modification du fuseau horaire nécessite le redémarrage du firewall.
- Pour permettre au firewall de synchroniser son horloge automatiquement avec un serveur NTP, il suffit de cocher l'option Maintenir le firewall à l'heu□e (NTP). Par défaut, deux serveurs NTP appartenant à Stormshield sont préconfigurés dans la liste des serveurs. Cette liste peut être modifiée.



2. ADMINISTRATION DU FIREWALL :

- Il est possible de ne plus autoriser le compte « admin » à accéder à l'interface d'administration. Cela implique qu'un nouvel administrateur ait été préalablement créé avec des droits suffisants. Dans le contraire, l'accès à l'interface d'administration par ce compte admin ne pourra être restauré que par une modification de configuration en mode commande.

- Le port utilisé pour accéder à l'interface d'administration du firewall peut être un autre port que le standard HTTPS (443/TCP), défini par défaut. L'URL d'accès devient alors : *https://@IP_firewall:port/admin*.
- Par défaut, l'interface d'administration du firewall utilise un certificat issu de l'autorité de certification du firewall. Le lien « Configurer le certificat SSL pour l'accès à l'interface d'administration » renvoie vers le menu qui permet de modifier ce certificat.
- Le délai maximal d'inactivité peut être défini pour tous les administrateurs. Un administrateur peut configurer un temps de déconnexion en cas d'inactivité dans ses préférences (menu accessible en cliquant sur son nom utilisateur), si ce temps de déconnexion est inférieur ou égal au délai maximal paramétré.
- La protection contre les attaques force brute pour l'accès à l'interface d'administration peut être activée/désactivée et le nombre de tentatives ainsi que le temps d'attente (en minutes) sont paramétrables. Par défaut, après 3 tentatives d'authentification infructueuses, l'accès depuis cette adresse IP sera bloqué pendant 1 minute.

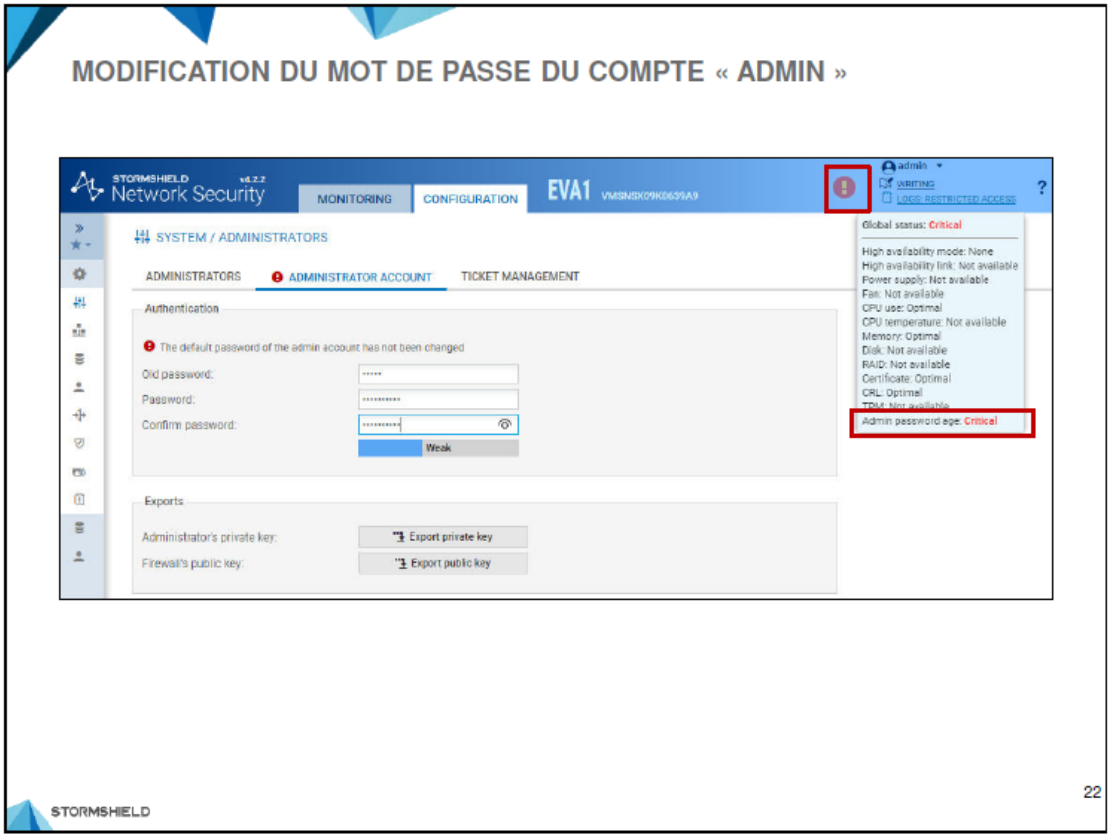


3. PARAMÈTRES RÉSEAUX :

- Les firewalls Stormshield Network supportent le protocole IPv6 et plusieurs fonctionnalités (interface, routage, filtrage, VPN et administration) sont compatibles IPv6. Cependant, ce support est optionnel et son activation s'effectue via le bouton Activer le support du protocole IPv6 sur ce Firewall.
- Dans le cas où le firewall transite par un proxy pour accéder à Internet, les paramètres se renseignent depuis ce menu.
- Un ou plusieurs serveurs DNS peuvent être ajoutés. Le firewall contacte ces serveurs pour toute résolution □u'il émet ou doit relayer. Ces résolutions de noms sont nécessaires pour des fonctionnalités telles que Active Update qui interroge les serveurs de mise à jour pour télécharger les bases de données

(signatures contextuelles, antivirus, Vulnerability Manager, …). Ces serveurs DNS sont également utilisés dans le cas où le service cache DNS est activé en mode transparent (voir annexe Proxy cache DNS).

Modification du mot de passe du compte « admin »



Tant que le mot de passe de la configuration usine n'a pas été modifié, une erreur critique est affichée dans l'en-tête de l'interface d'administration (encadrés rouges). Le mot de passe du compte « admin » doit être modifié dans l'onglet COMPTE ADMIN du menu CONFIGURATION ⇒ SYSTÈME ⇒ Administrateurs. Le mot de passe doit avoir au minimum 5 caractères et doit respecter la politique de mot de passe définie dans le menu CONFIGURATION.