Le site https://documentation.stormshield.eu est accessible sans authentification. Il contient l'ensemble des documentations publiques gérées par l'équipe des rédacteurs technique Stormshield:

- Notes de versions,
- Guides de configuration,
- Notes techniques.

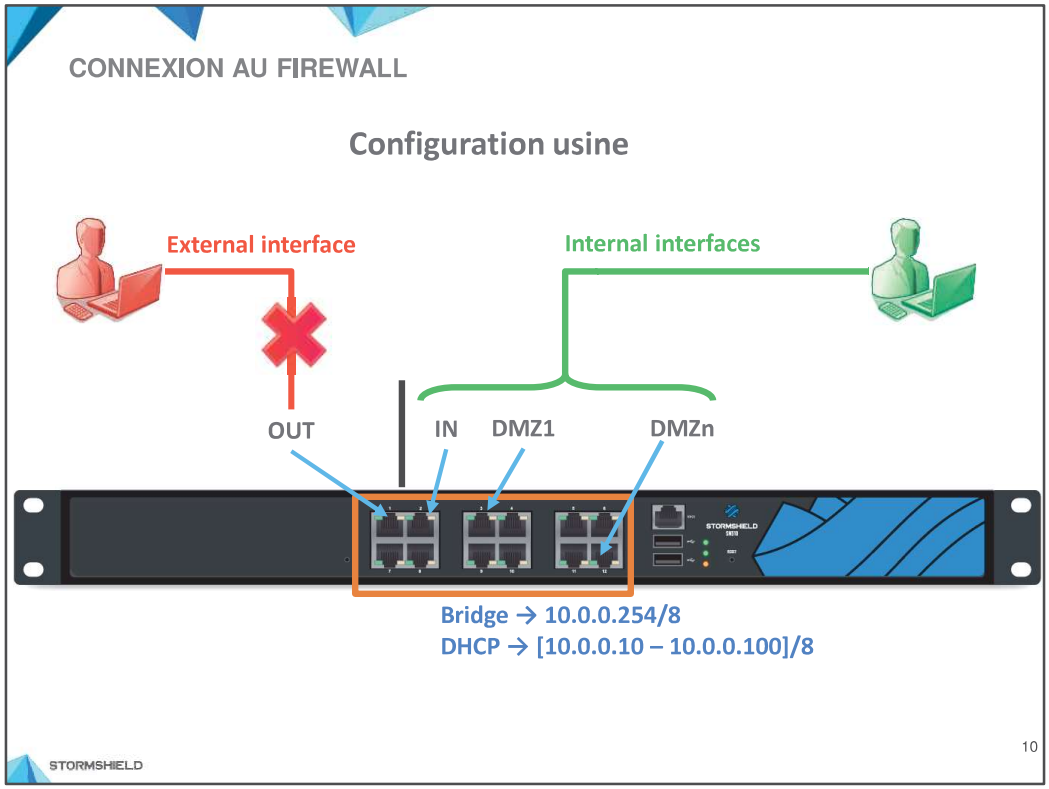
Ce dernier type de document vous permet de mettre en place des configurations évoluées grâce à une présentation pas à pas des notions à maitriser et des paramètres à définir.

Il faut être certifié CSNE

La base de connaissance est accessible à l'URL https://kb.stormshield.eu. L'authentification à cette ressource est basée sur les identifiants MyStormshield. Cette base est alimentée et maintenue en permanence par l'équipe du TAC (support technique) SNS.

Vous y trouverez entre autre :

- Les paramètres de configuration spécifiques,
- La liste des limitations fonctionnelles connues,
- L'enregistrement des webinaires créés par le TAC,
- Les procédures de diagnostics.



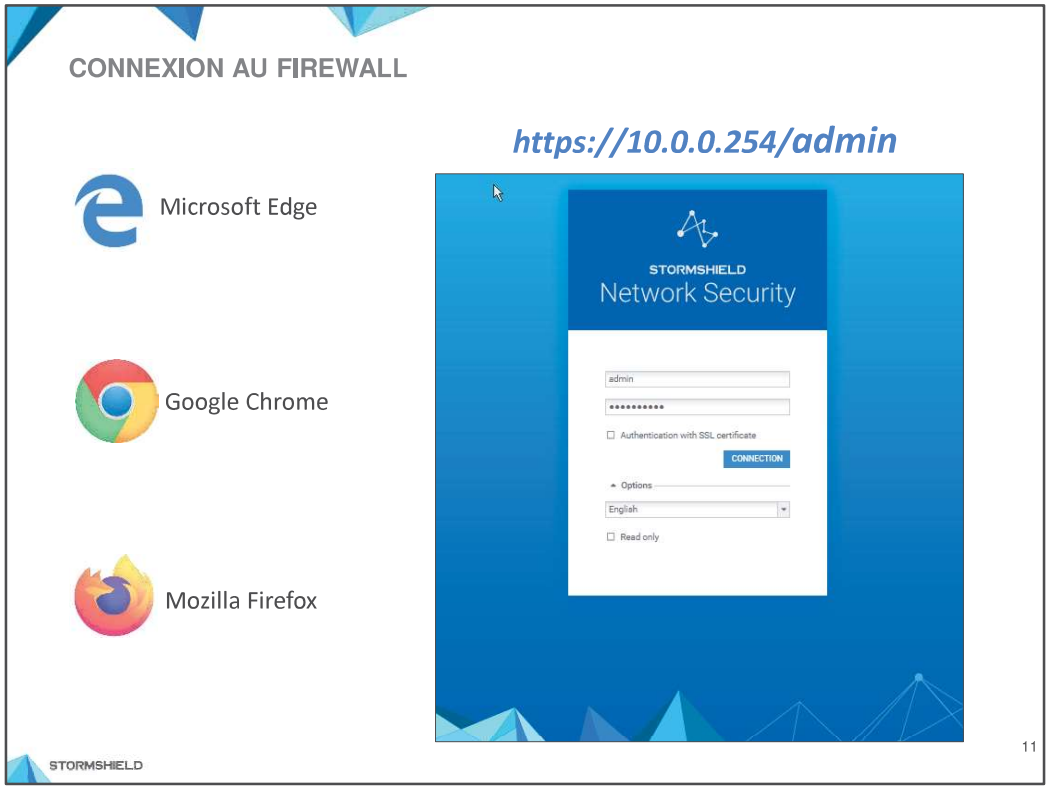
Dans une configuration usine, la première interface du firewall est nommée « OUT », la seconde « IN » et le reste des interfaces « DMZx ». L'interface « out » est une interface externe, utilisée pour connecter le firewall à internet et le reste des interfaces sont internes et servent principalement à connecter le firewall à des réseaux locaux.

La distinction interne/externe pour les interfaces 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.

Pour accéder à l'interface d'administration du firewall, vous devez connecter votre machine sur une interface interne.

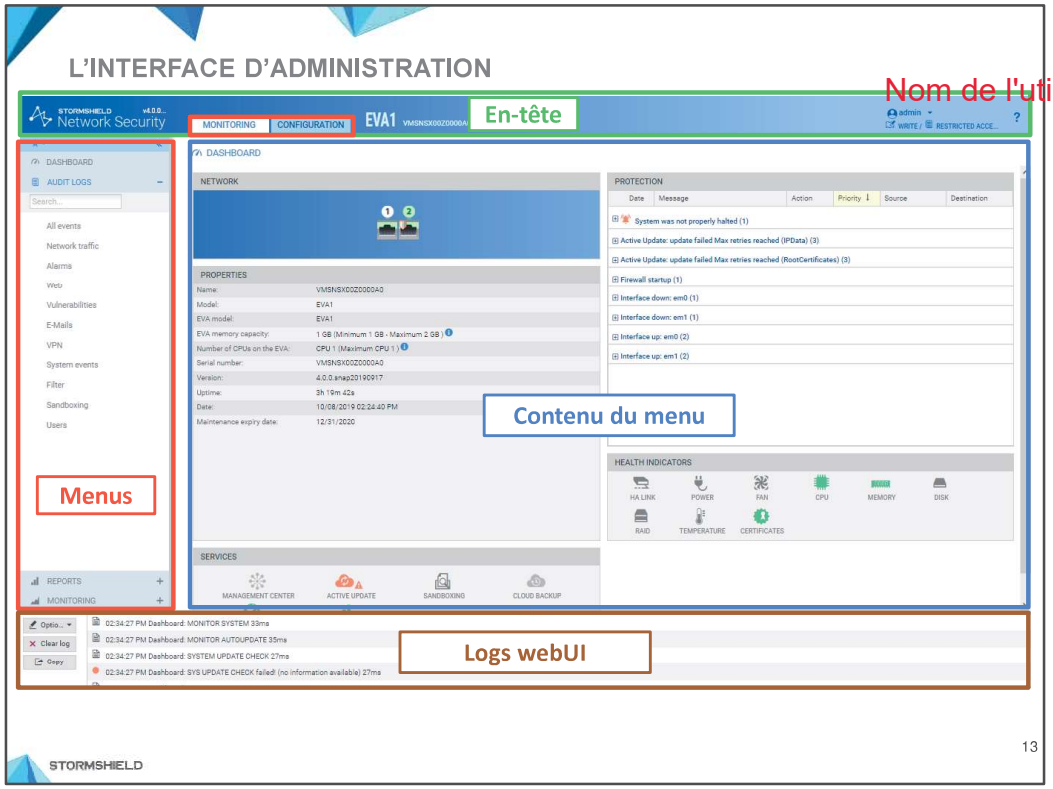
NOTE : Avec la configuration usine, connecter une machine sur l'interface externe et ensuite sur une interface interne sera interprété par le firewall comme une tentative d'usurpation d'adresse IP sur le bridge et par conséquent, il bloquera tout le trafic généré par cette machine. Le redémarrage du firewall sera nécessaire pour débloquer cette situation.



L'accès à l'interface graphique d'administration du firewall s'effectue grâce à un navigateur Web en HTTPS à l'adresse « *https://10.0.0.254/admin* ». Pour un fonctionnement optimal de cette interface, il est recommandé d'utiliser la dernière version des navigateurs Microsoft Edge, Google Chrome et Mozilla Firefox

L'accès aux pages d'administration nécessite une authentification. Par défaut, seul le compte système **admin**, disposant de tous les privilèges sur le boitier, existe et peut se connecter. En configuration usine, le mot de passe de ce compte est également **admin**; pour des raisons évidentes de sécurité, il conviendra de modifier ce mot de passe.
Pour s'authentifier, l'utilisateur peut également sélectionner un certificat dans le magasin de son navigateur.

Dans les options avancées, l'administrateur peut choisir la langue des menus de configuration ainsi que l'accès en en lecture seule, ce qui empêche toute modification de la configuration.
En haut à droite de la page, l'icône suivante permet d'accéder au menu d'aide en ligne ?



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

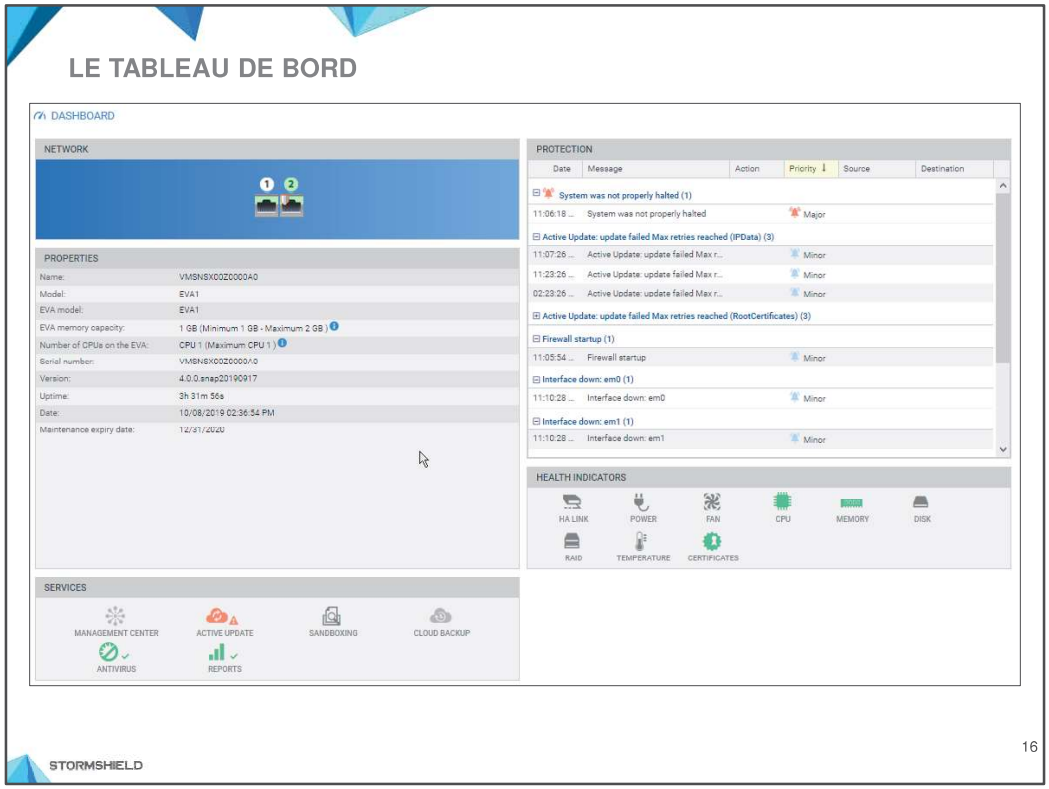
1. **L'en-tête (partie encadrée en vert) :** Elle contient les informations suivantes :
   - Le nom du firewall: le nom par défaut est le numéro de série,
   - La version du système (firmware),
   - L'utilisateur connecté sur l'interface, ses droits d'accès à la configuration: lecture seule ou écriture 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.

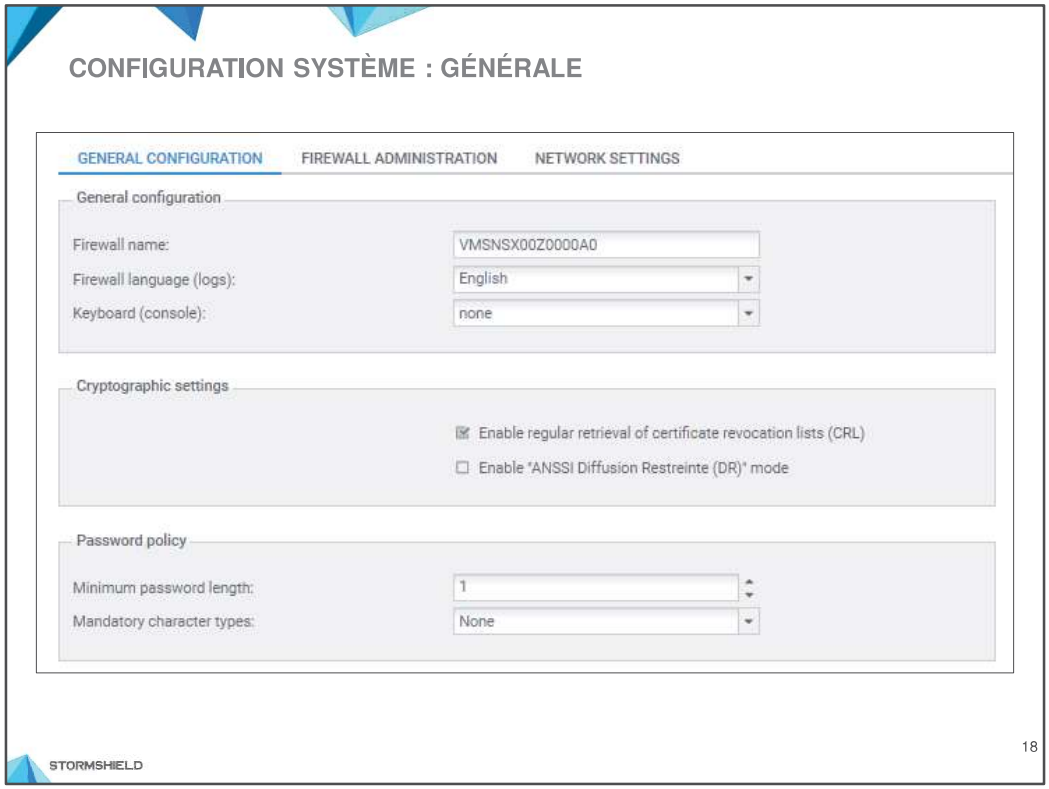
4. **Les logs de la webUI (partie encadrée en marron) :** Affiche une liste (paramétrable) des logs de l'interface web. On peut y faire apparaitre par exemple les commandes NSRPC exécutées par l'interface web, les erreurs levées, les avertissements, ….



Le tableau de bord, regroupe l'ensemble des informations et indicateurs du firewall :

- 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.

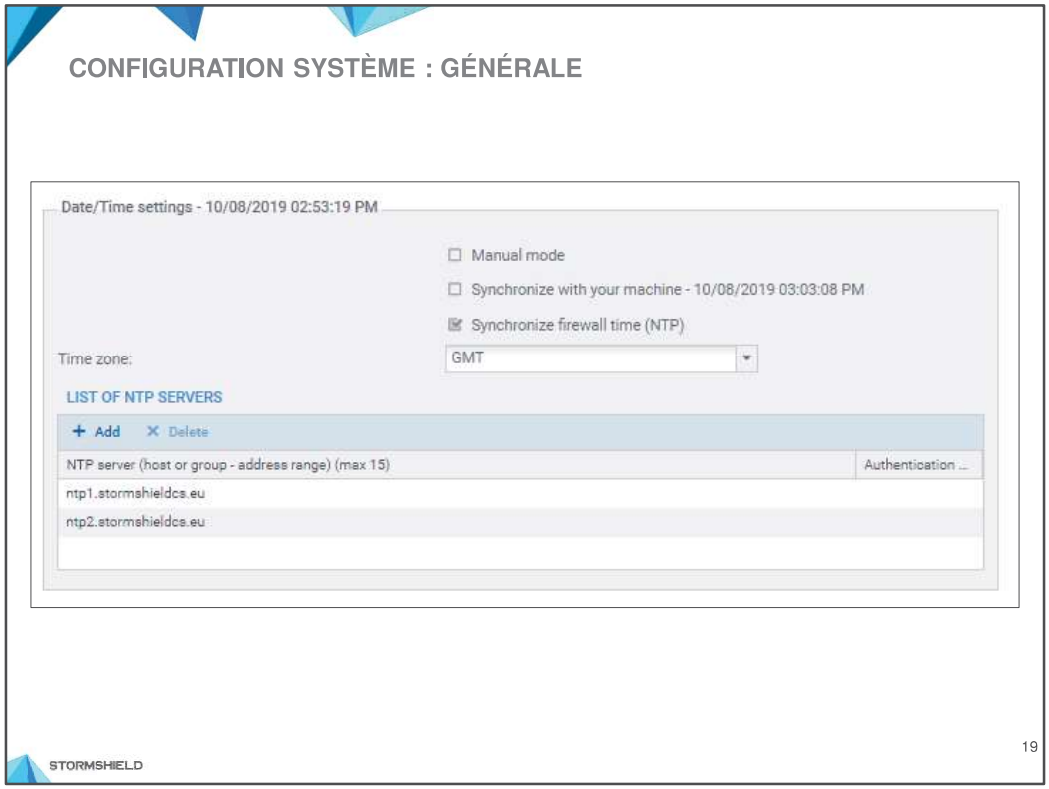
Un clic sur un élément du tableau de bord renvoie directement vers la page de supervision ou de configuration liée à cet élément.



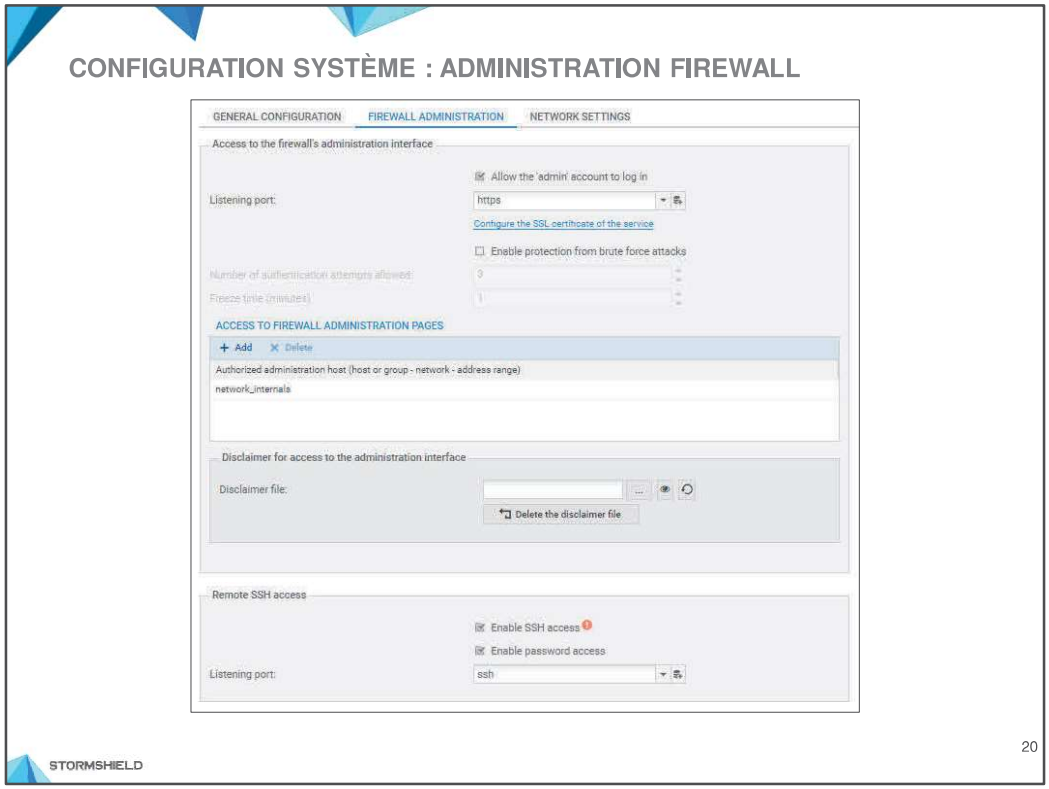
Le menu **CONFIGURATION ⇒ SYSTÈME ⇒ Configuration** permet de configurer les paramètres systèmes, administratifs et réseaux du firewall. Il est composé de trois onglets :

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 ».
- La politique de mots de passe définit la longueur minimale et les caractères obligatoires des mots de passe créés dans les différents menus du firewall (par exemple : mots de passe des utilisateurs dans l'annuaire interne (LDAP), mots de passe qui protège les fichiers de sauvegarde, mots de passe des certificats créés au niveau du firewall). Par défaut, la longueur minimale est à un et aucun caractère n'est obligatoire. Cependant, l'administrateur peut imposer des mots de passe alphanumérique seulement ou alphanumérique avec des caractères spéciaux.



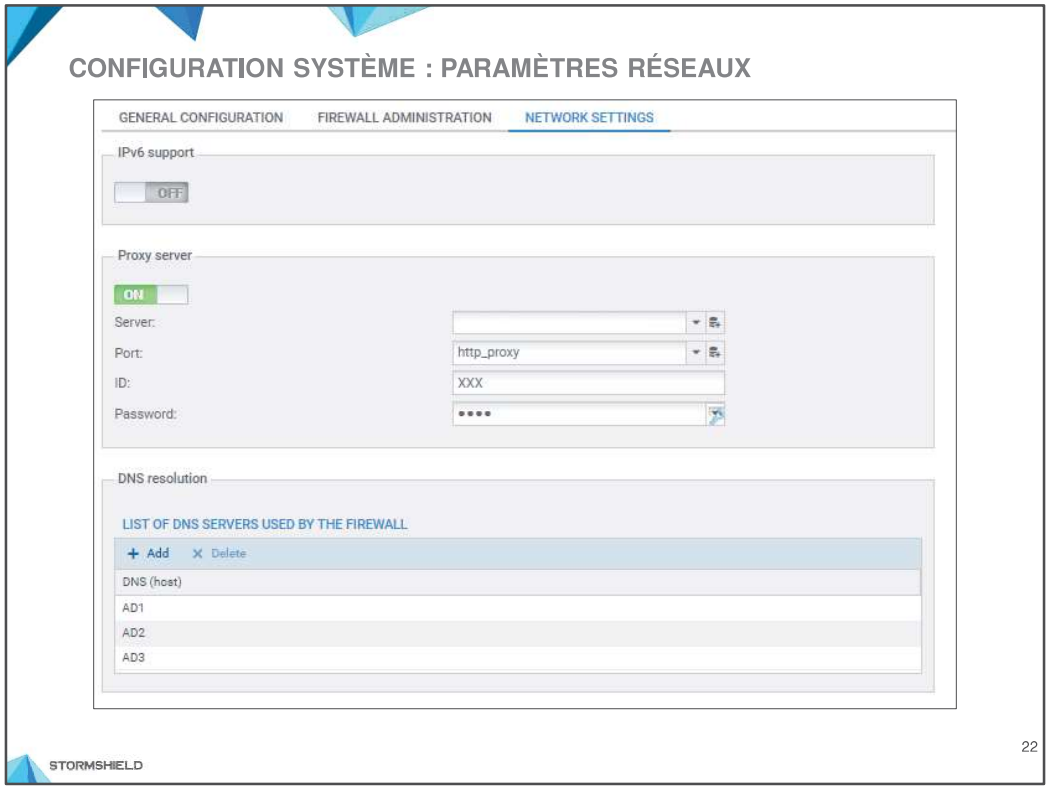
- Les paramètres horaires: date, heure et fuseau horaire. Ces paramètres sont cruciaux pour des fonctionnalités telles que les logs ou l'authentification. La modification du fuseau horaire nécessite le redémarrage du firewall.
- Pour permettre au firewall de synchroniser son horloge automatiquement avec un serveur NTP, il suffit de cocher l'option Maintenir le firewall à l'heure (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 créé avec des droits suffisants. Dans le cas contraire, vous perdrez définitivement l'accès à l'interface d'administration du firewall.
- 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.
- 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.
- L'accès à l'interface d'administration peut être limité à une machine ou un réseau spécifique. Dans ce cas, la machine ou le réseau doit apparaître dans la liste « Poste d'administration autorisé ». Par défaut, seuls les réseaux internes et représentés par l'objet « Network_internals » sont autorisés à y accéder.

- Il est possible d'activer l'accès par SSH (connexion sécurisée) et de modifier le port d'écoute du service qui est par défaut SSH (22/TCP). L'activation du mot de passe est nécessaire pour un accès simplifié. Dans ce cas, l'utilisateur est invité à saisir un login et un mot de passe lors de la connexion. Dans le cas contraire, vous êtes obligés de gérer les accès par une paire de clés.



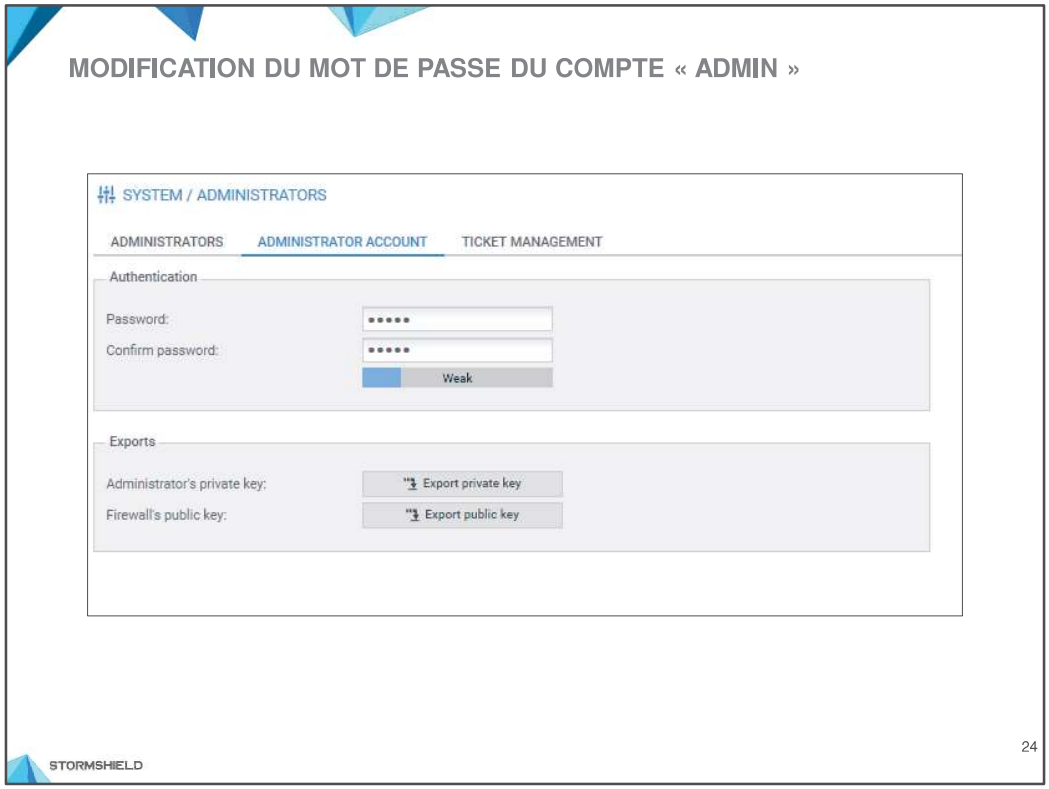
3. PARAMÈTRES RÉSEAUX :

- 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**.

  NOTE : Cette action étant irréversible, la sauvegarde de la configuration du firewall vous sera proposée automatiquement lorsque vous cliquerez sur ce bouton. Le retour à un support IPv4 exclusif (sans IPv6) n'est possible qu'après une remise à la configuration usine (reset) du firewall.

- Dans le cas où le firewall transite par un proxy pour accéder à Internet, les paramètres se renseignent depuis ce menu.

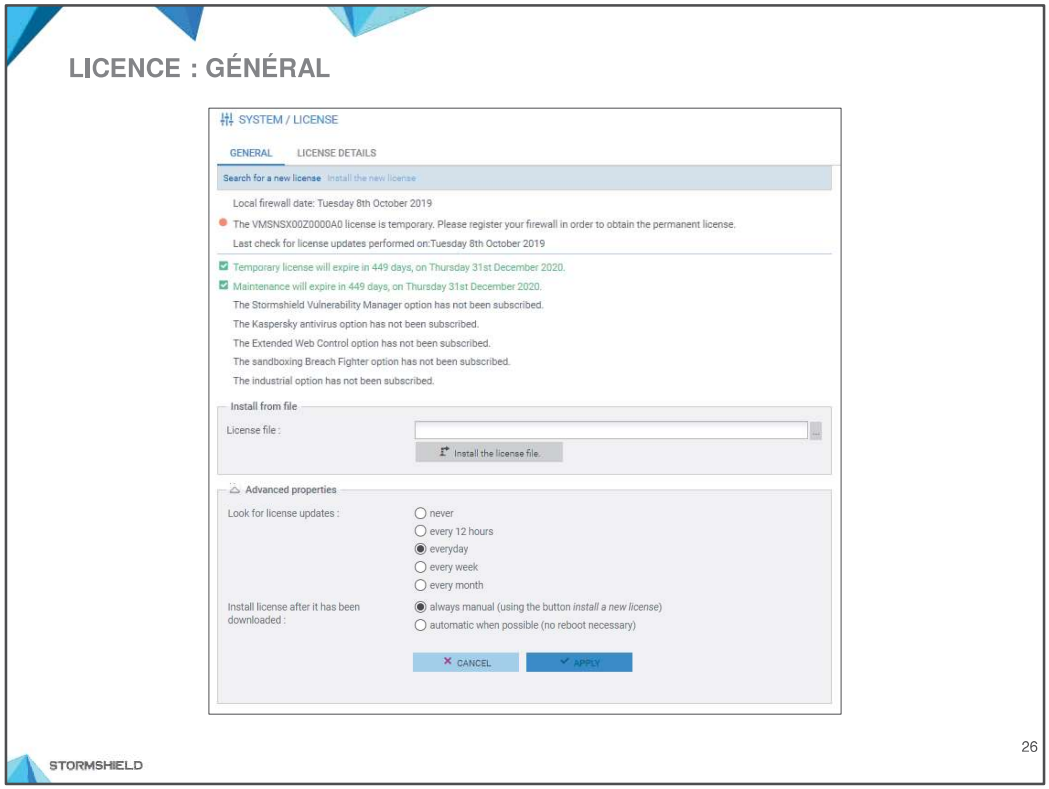
- Un ou plusieurs serveurs DNS peuvent être ajoutés. Le firewall contacte ces serveurs pour toute résolution qu'il émet ou doit relayer. Ces résolutions de noms sont nécessaires pour des fonctionnalités telles que Active Update qui interroge les serveurs de mise à jour pour télécharger les bases de données (signatures contextuelles, antivirus, Vulnerability Manager, ...). Ces serveurs DNS sont également utilisés dans la cas où le service cache DNS est activé en mode transparent (voir Annexe Proxy cache DNS).



Le mot de passe du compte « admin » peut 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**.

La force du mot de passe indique son niveau de sécurité : Très faible, faible, moyen, bon, excellent. Il est fortement conseillé d'utiliser les majuscules et les caractères spéciaux pour augmenter le niveau de sécurité.

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.

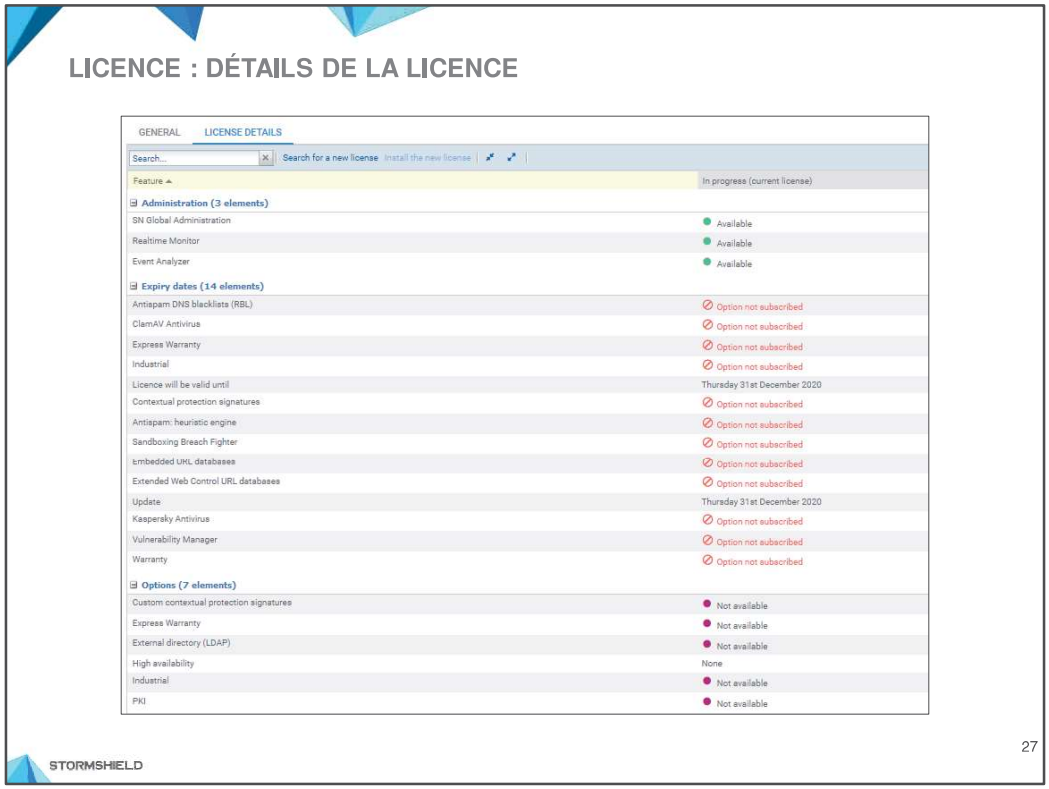


Le menu **CONFIGURATION ⇒ SYSTÈME ⇒ Licence**, affiche toutes les informations concernant la licence. Le firewall possède une licence temporaire valide 3 mois, permettant son fonctionnement immédiatement après sa mise en marche. La licence définitive est à télécharger depuis votre espace privé Stormshield (après enregistrement du firewall) ou à installer automatiquement. Elle se présente sous la forme d'un fichier « .licence ».

Le menu est constitué de deux onglets:

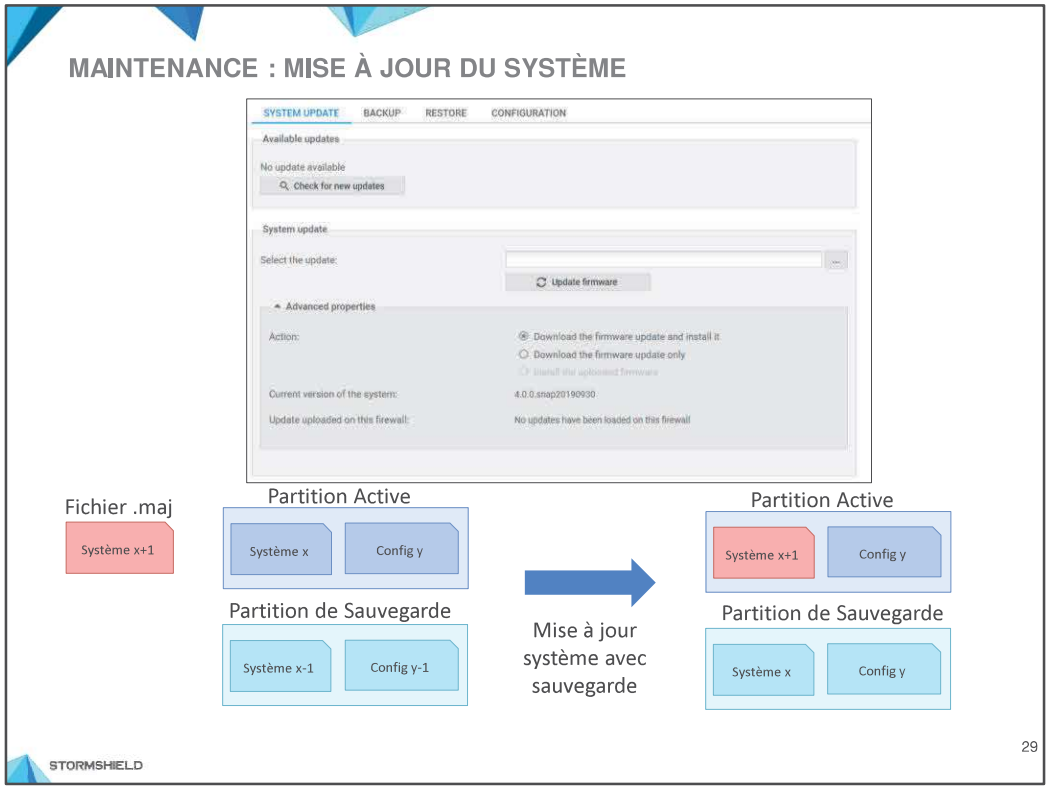
1. GÉNÉRAL :

En haut de l'onglet un bouton permet de rechercher les nouvelles licences directement sur les serveurs de mise à jour Stormshield et un autre bouton permet de l'installer. Ils sont suivis d'informations sur la durée de validité de la licence et des différentes options disponibles. La partie **Installation à partir d'un fichier** permet d'installer la licence à partir du fichier « .licence » stocké sur le PC.
Enfin, la partie **Configuration avancée** permet de configurer la fréquence de recherche des mises à jour et également d'en automatiser l'installation.



2. DÉTAILS DE LA LICENCE :

Les boutons de recherche et d'installation de la licence sont également présents ici.
Une barre de recherche permet de trouver rapidement la disponibilité d'une option ou d'un service dans la licence.
Le reste de la page détaille le contenu de la licence avec les durées de validité.



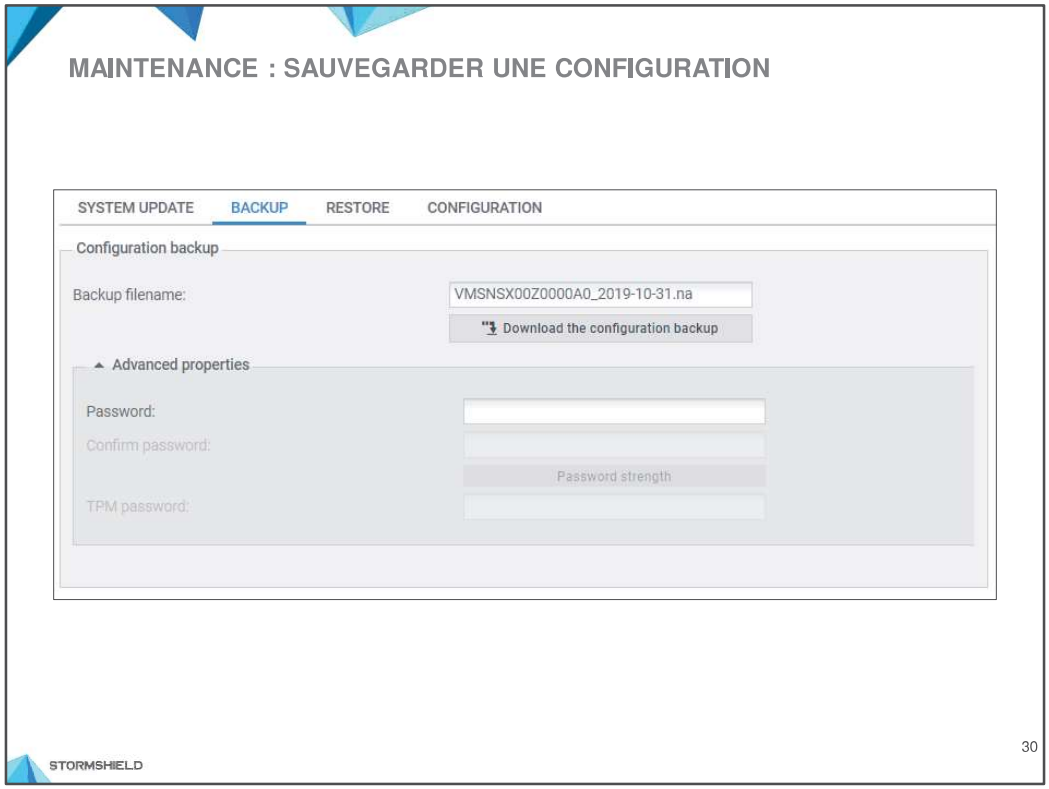
Le menu **CONFIGURATION ⇒ SYSTÈME ⇒ Maintenance** permet de gérer les mises à jour système ainsi que les sauvegardes/restaurations de configuration. Quatre onglets composent ce menu:

1. Mise à jour du système :

Cet onglet permet à l'administrateur de mettre à jour la version du système (firmware). Le fichier de mise à jour « .maj » peut être téléchargé au niveau du compte client Stormshield ou bien récupéré automatiquement par le firewall en appuyant sur le bouton « Recherche de nouvelles mises à jour ».

La figure ci-dessus illustre la mise à jour du système des partitions. La nouvelle version du système « x+1 » remplacera l'ancienne version « x » se trouvant sur la partition active tout en gardant la même configuration « y ». L'administrateur peut choisir ou non de faire une sauvegarde de la partition active sur la partition de sauvegarde, avant la mise à jour, grâce à l'option « Sauvegarder la partition active sur la partition de sauvegarde avant de mettre à jour le firewall » (Si l'option est cochée, l'ancienne version du système « x-1 » et la configuration « y-1 » seront définitivement perdues).

Dans la « configuration avancée », l'administrateur peut choisir de télécharger et d'activer une mise à jour ou bien de la télécharger uniquement, son activation pourra se faire ultérieurement avec l'option « Activer le firmware précédemment téléchargé ».

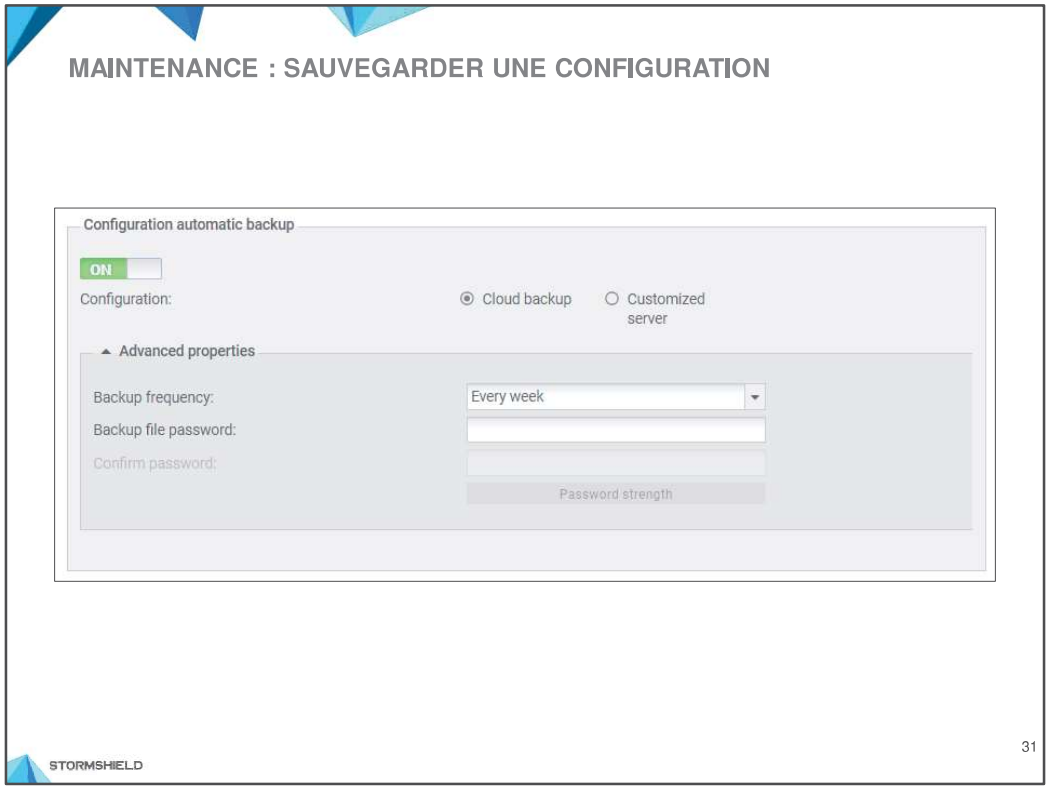


2. SAUVEGARDER :

Dans cet onglet, l'administrateur peut effectuer une sauvegarde manuelle de la configuration du firewall qui est téléchargée et enregistrée sous le format d'un fichier chiffré « .na ». Les éléments sauvegardés dans le fichier sont listés ci-dessous:

- Réseau (interface, routage et DNS dynamique),
- Filtrage SMTP,
- Filtrage URL,
- Filtrage SSL,
- Objets web,
- Modules globaux,
- Configuration sécurisée,
- Active Update,
- Services (SNMP, serveur DHCP),
- Profils d'inspection IPS,
- Objets réseaux,
- Filtrage et NAT,
- VPN IPSec,
- Annuaire LDAP.

L'administrateur ne peut pas sauvegarder une partie de la configuration via l'interface web (une sauvegarde partielle est possible en ligne de commande). Le fichier peut être protégé en plus par un mot de passe qui doit être renseigné, avant le téléchargement, dans la partie « configuration avancée ».



L'administrateur peut également activer la sauvegarde automatique du fichier de configuration. Deux options sont possibles :

- Cloud backup : En activant cette option, le fichier de configuration est stocké sur un serveur hébergé dans une infrastructure de service nommée « cloud backup service » gérée par Stormshield. La sauvegarde peut être effectuée chaque jour, chaque semaine ou chaque mois. Dans la « configuration avancée », on peut configurer cette fréquence et protéger la configuration par un mot de passe grâce aux paramètres « Fréquence des sauvegardes » et « Mot de passe du fichier de sauvegarde ». La sauvegarde est sécurisée avec une connexion HTTPS et une authentification par certificat. Au maximum, 5 fichiers de configuration par firewall peuvent être sauvegardés sur les serveurs du cloud. Au-delà, le nouveau fichier écrasera le plus ancien. Ces fichiers sont accessibles depuis l'espace client Stormshield.

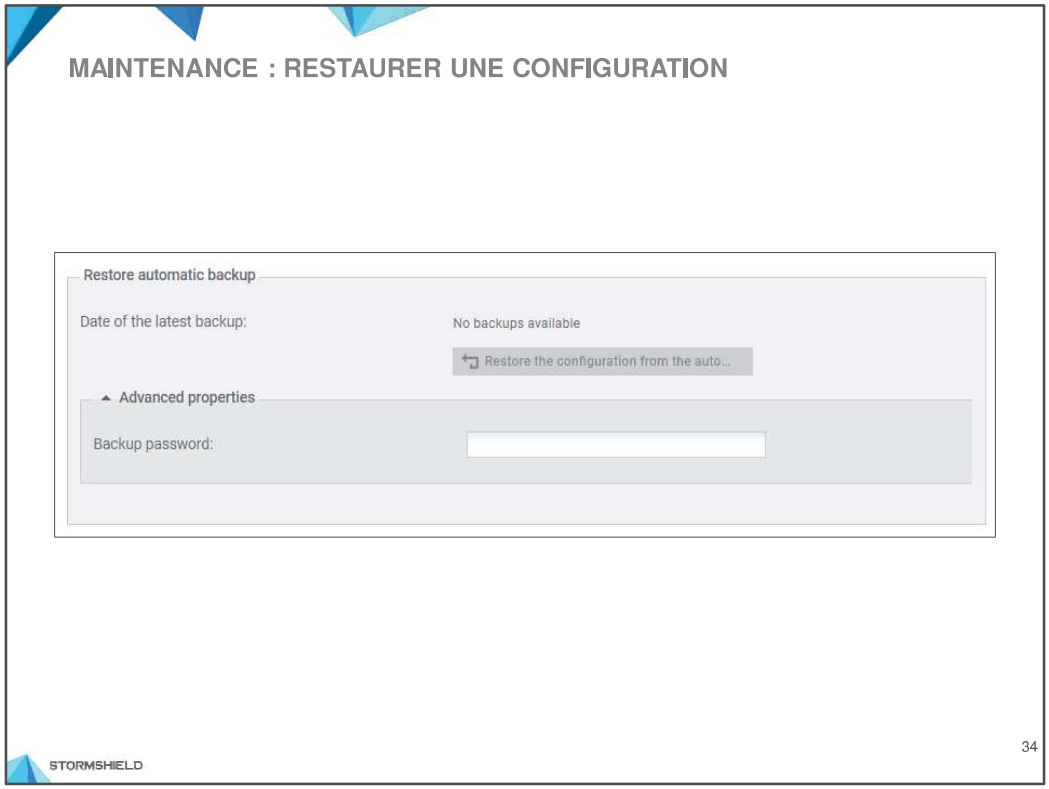
- Serveur personnalisé : Avec cette option les fichiers de configuration sont stockés sur un serveur dont l'adresse IP est renseignée dans le paramètre « Serveur de sauvegarde ». Plusieurs paramètres peuvent être configurés dans la « configuration avancée » :
  - « Port du serveur »: port d'écoute du serveur de sauvegarde,
  - « protocole de communication »: HTTP ou HTTPS,
  - « Certificat du serveur »: actif uniquement si le protocole HTTPS est choisi. Il permet de spécifier le certificat présenté par le serveur sur lequel sera envoyée la sauvegarde de configuration. L'objectif est que le firewall puisse s'assurer de l'identité du serveur avant de lui transmettre le fichier de sauvegarde,
  - « Chemin d'accès »: Permet de spécifier le répertoire où seront stockés les fichiers de configuration,
  - « Méthode d'envoi »: Permet de choisir la méthode d'envoi HTTP : authentification basic (auth basic) , authentification digest (auth digest) ou POST,
  - « Identifiant » et « Mot de passe »: Utilisés avec les méthodes d'envoi « auth basic » et « auth digest »,
  - « POST – control name »: Utilisé avec la méthode d'envoi POST,
  - « Fréquence des sauvegardes »: fréquence d'envoi des sauvegardes positionnée par défaut à une semaine,
  - « Mot de passe du fichier de sauvegarde »: protège les fichiers de sauvegarde par un mot de passe.

3. RESTAURER :

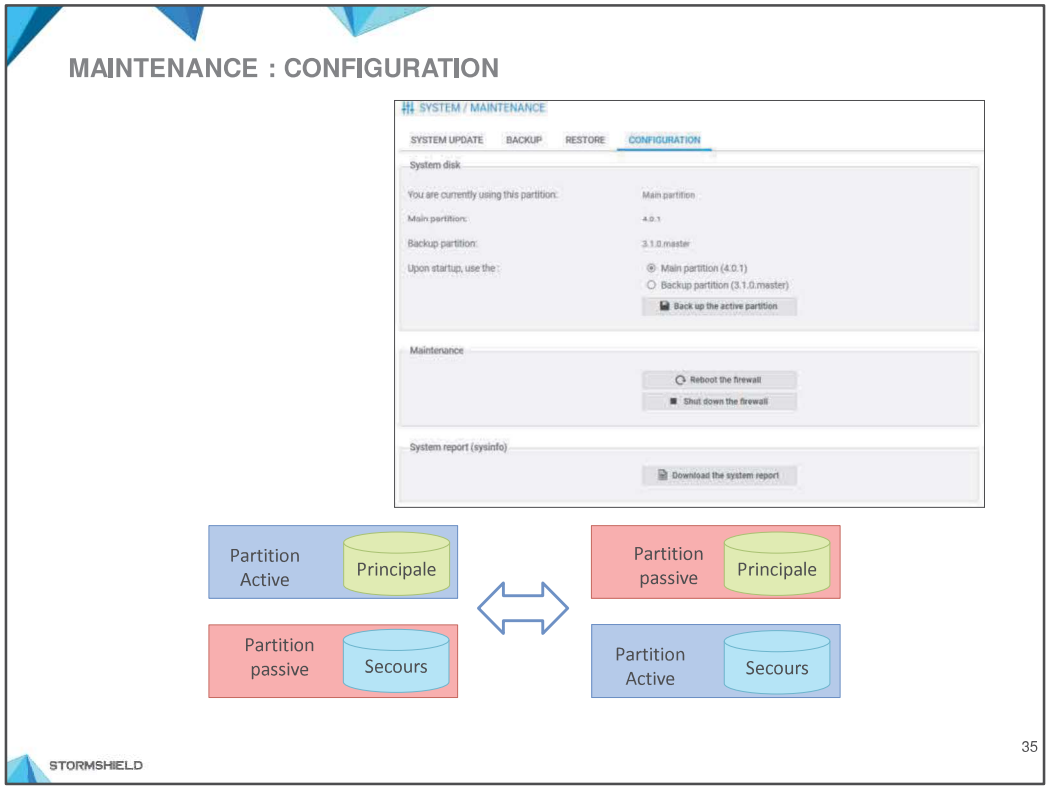
La restauration d'une configuration s'effectue à partir d'un fichier « .na » stocké sur la machine. Si le fichier de configuration est protégé par un mot de passe, l'administrateur doit le saisir dans la partie « configuration avancée ».

En fonction des besoins, seule une partie de la configuration peut être restaurée. Dans ce cas, dans la partie *Configuration avancée,* sélectionnez le ou les modules nécessaires. Dans tous les cas, il est conseillé de redémarrer le firewall après une restauration (le redémarrage est proposé uniquement après une restauration complète).

NOTE : Le mot de passe de l'utilisateur « admin » n'est pas contenu dans le fichier de configuration. Il ne sera donc ni restauré, ni sauvegardé.



La restauration d'une configuration peut également se faire à partir de la dernière sauvegarde automatique dont la date est indiquée par « **Date de la dernière sauvegarde** ». Dans le cas où la sauvegarde est protégée par un mot de passe, ce dernier doit être renseigné dans la « configuration avancée ».

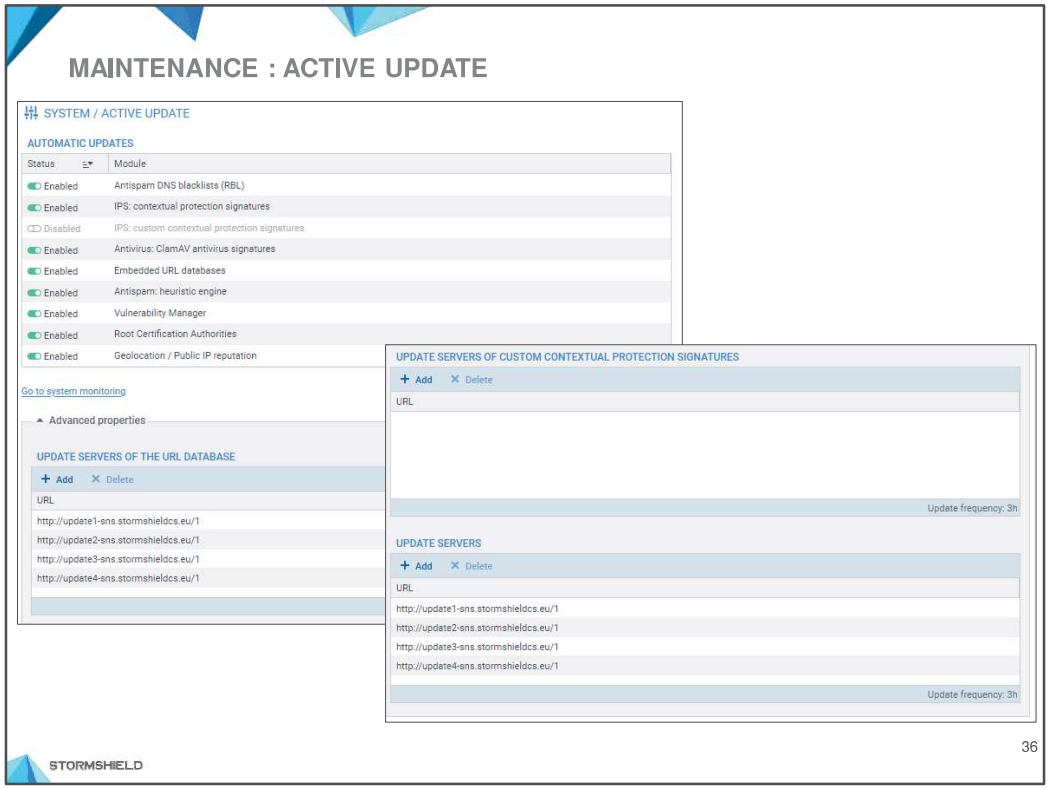


4. CONFIGURATION :

Tous les UTM physiques Stormshield Network disposent de deux partitions complètement indépendantes qui permettent le stockage de versions de firmware différentes. Chaque partition possède sa propre configuration. Il faut faire la distinction entre les partitions principale/secours et les partitions active/passive. Nous pouvons avoir deux cas de figure illustrés ci-dessus : (1) partition active => principale et partition passive=>secours ou (2) partition active => secours et partition passive => principale.

L'administrateur peut sélectionner la partition qui deviendra active au prochain démarrage du firewall (principale ou de secours). Automatiquement l'autre partition deviendra la partition passive.
Le bouton « sauvegarder la partition active » permet de copier tout le contenu de la partition active (configuration + firmware) sur la partition de sauvegarde.

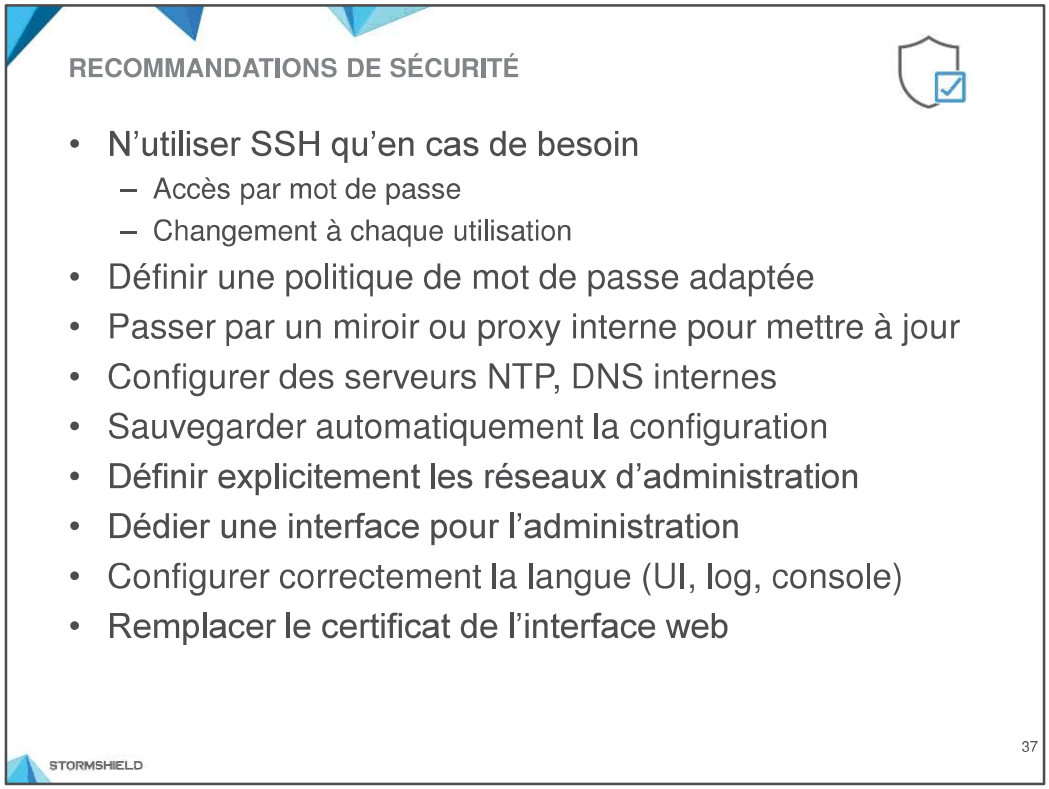
Les dernières options de maintenance permettent de redémarrer ou arrêter le firewall et de télécharger le rapport système: fichier texte qui affiche l'état du firewall et de nombreux autres indicateurs utiles au diagnostic par le support technique.



Le menu **CONFIGURATION ⇒ SYSTÈME ⇒ Active Update** permet de contrôler la mise à jour automatique des modules suivants :

- Antispam : listes noires DNS (RBL),
- Bases d'URLs embarquées,
- IPS : Signatures de protection contextuelles,
- Antivirus : signatures Antivirales ClamAV (ou Kaspersky),
- Antispam : moteur heuristique,
- Management de vulnérabilités (si l'option est active dans la licence),
- Autorités de certification racine.
- IPS : Signatures de protection contextuelle personnalisées.
- Géolocalisation / Réputation IP publiques.

L'administrateur peut activer ou désactiver la mise à jour d'un seul module ou de tous les modules à la fois en utilisant les boutons « Tout autoriser » ou « Tout refuser ».
Les listes des serveurs de mise à jour des différents modules et de la base d'URL sont accessibles dans la partie « configuration avancée ». L'administrateur peut modifier, ajouter ou supprimer des serveurs.



L'accès SSH se fait avec le compte admin, il doit donc être occasionnel et suivi. En dehors de ces cas, il doit être désactivé pour réduire la surface d'attaque. Le mot de passe devrait être changé à chaque fois.

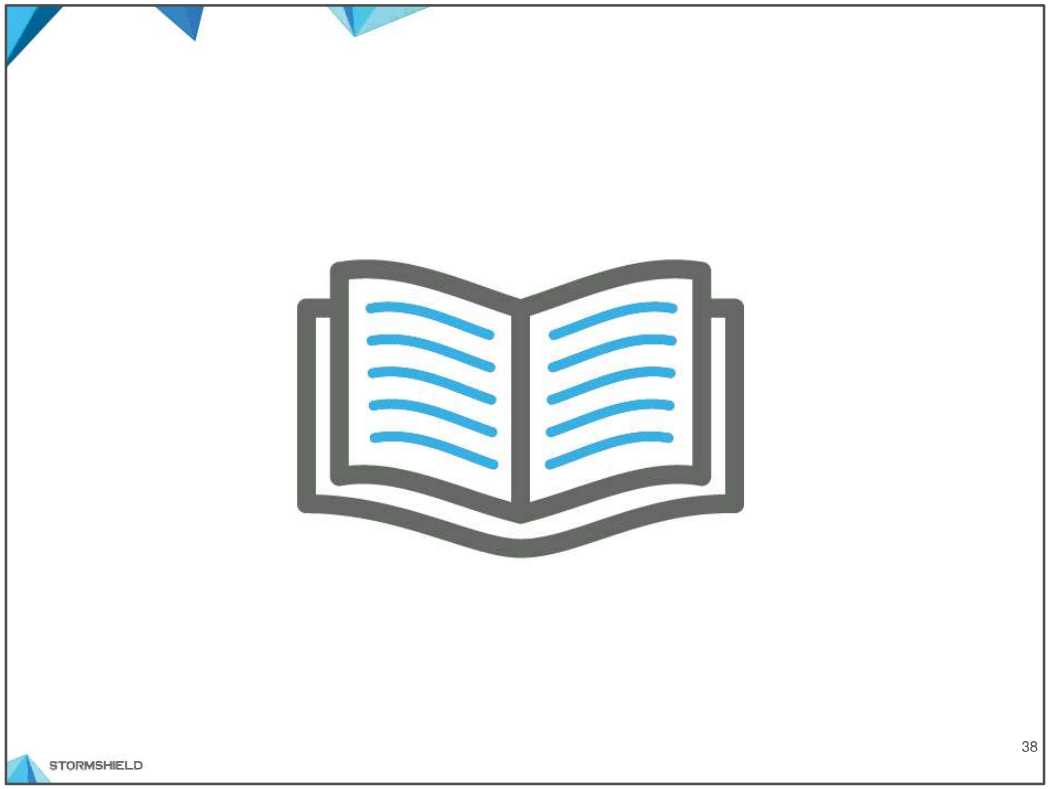
Un proxy ou un miroir interne permet de :
- Maitriser l'arrivée des mises à jour,
- Moins consommer de bande passante,
- Réduire le nombre de machines ayant accès à internet.

Un serveur NTP interne maintient la cohérence des dates dans les log du système d'information. C'est indispensable en vu de les corréler.
Un DNS interne permet de :
- Conserver la maitrise des résolutions de noms,
- Accélérer les résolutions.

L'administration du firewall doit se faire depuis un réseau protégé, identifié et totalement séparé de la production.

Les langues utilisées doivent être comprises par les utilisateurs afin de limiter les erreurs de manipulation du produit.

Sources des recommandations :
- https://www.ssi.gouv.fr/guide/recommandations-de-securisation-dun-pare-feu-stormshield-network-security-sns/
- https://www.ssi.gouv.fr/politique-filtrage-parefeu/
- https://www.ssi.gouv.fr/passerelle-interconnexion/



Pour aller plus loin, consultez les ressources du site documentation.stormshield.eu :

- Manuel d'utilisation et de configuration SNS
- Notes techniques:
    - Configuration initiale par clé USB
    - Sauvegardes automatiques
    - Restauration logicielle par clé USB
    - EVA sur Amazon Web Services
    - EVA sur Microsoft Azure

Et pour les situations/questions très spécifiques, consultez la base de connaissance du TAC kb.stormshield.eu.