PROCEDURE D'INSTALLATION : MAINTENANCE STORMSHIELD

PROJET

CUB

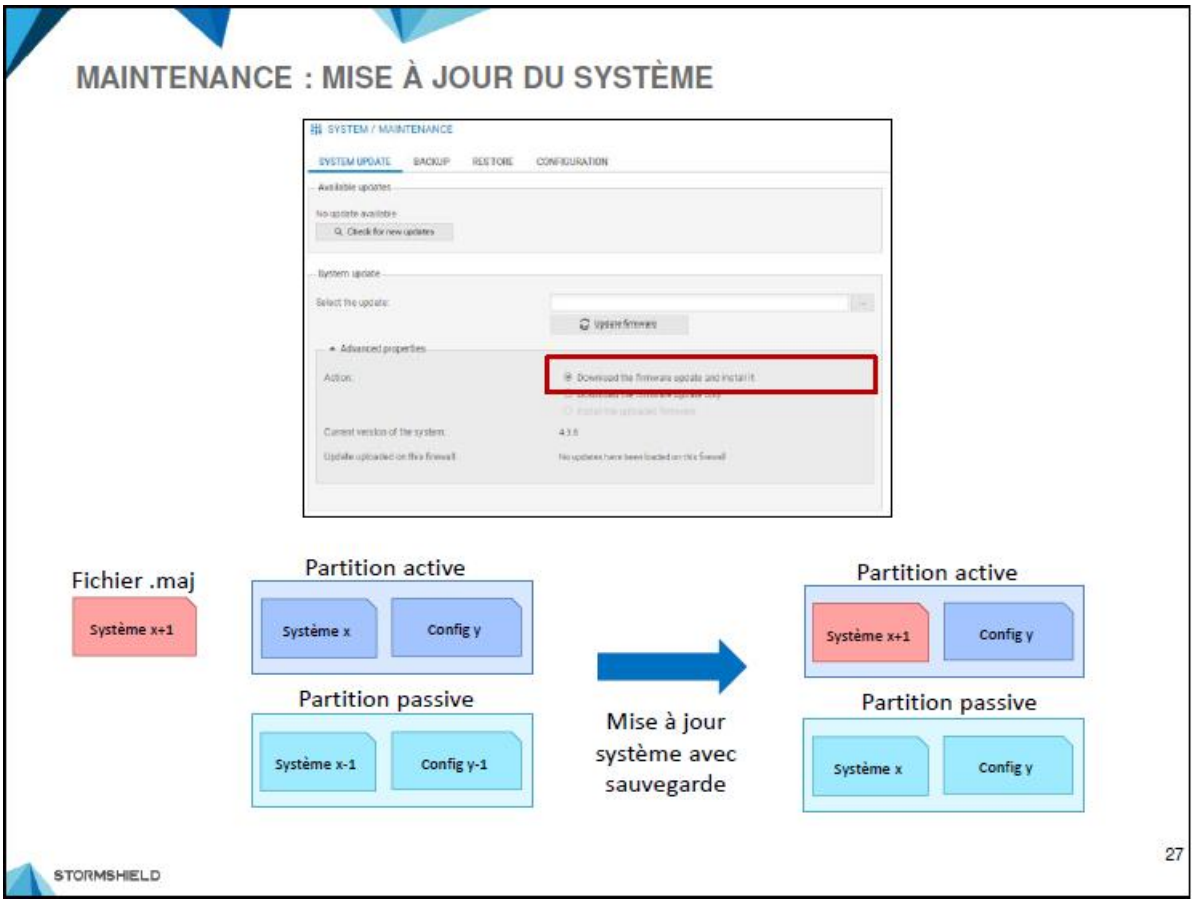
- **Objectif :** Assurer la sécurité du réseau via le filtrage du trafic, le chiffrement des communications (VPN), la gestion sécurisée, la surveillance des événements et la sauvegarde des configurations, afin de garantir la confidentialité, l'intégrité et la disponibilité des systèmes.

- **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

Maintenance



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 :

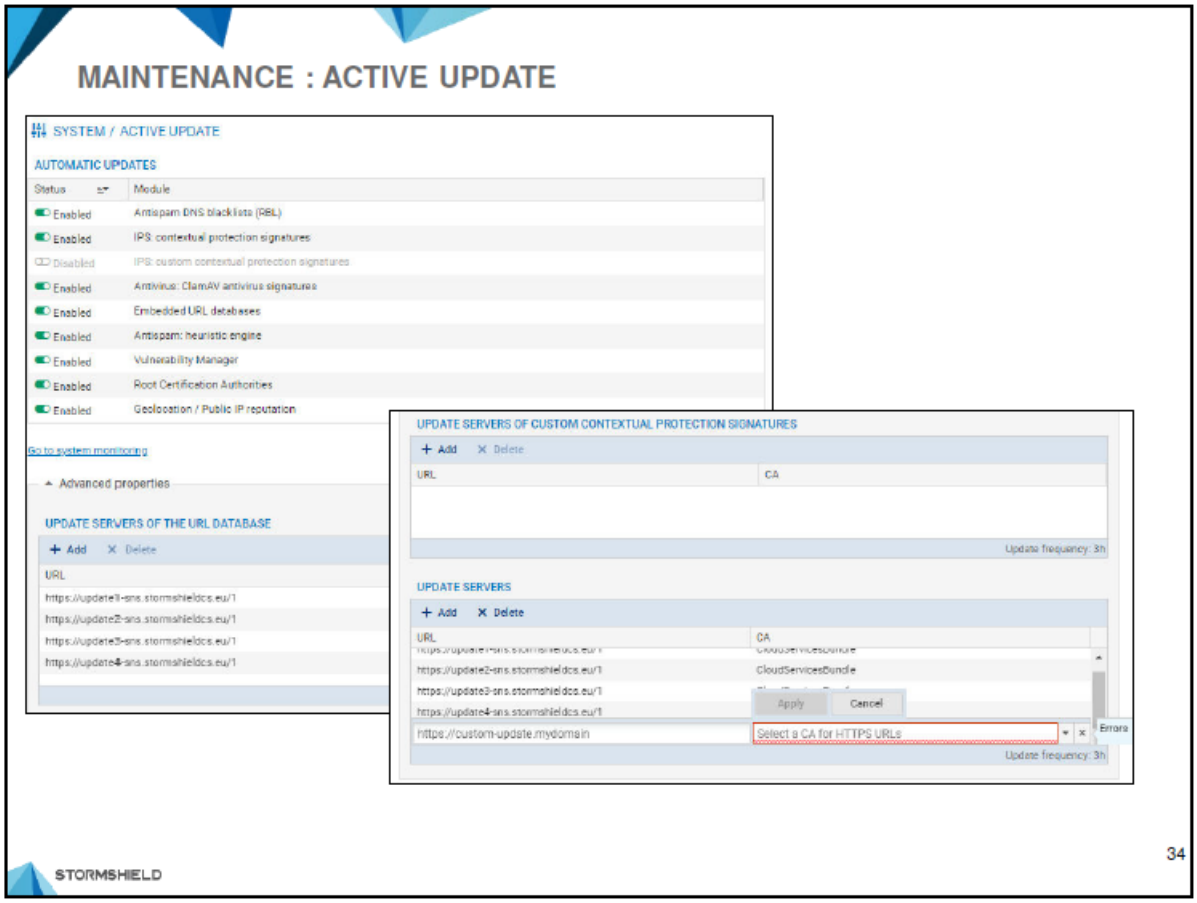
1. **Mise à jour système :**
   - Cet onglet permet à l'administrateur de mettre à jour la version du système (firmware). Le fichier de mise à jour « .maj » peut être téléchargé au niveau du compte client Stormshield ou bien récupéré automatiquement par le firewall en appuyant sur le bouton « Recherche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

   - La figure ci- dessus décrit la mise à jour du système des partitions (partie encadrée en rouge). La nouvelle version « x+1 » remplacera l'ancienne version « x » sur la partition active, tout en conservant la même configuration « y ». L'administrateur peut choisir de sauvegarder la partition active sur la partition de sauvegarde avant la

mise à jour. Si cette option est sélectionnée, l'ancienne version « 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 ».

Active Update



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 antivirus avancé),
- Antispam : moteur heuristique,
- Management de vulnérabilités (si l'optio 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'u 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'administration peut modifier, ajouter ou supprimer des serveurs.