

**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

**MAINTENANCE : MISE À JOUR DU SYSTÈME**

The screenshot shows the 'SYSTEM / MAINTENANCE' interface with tabs for 'SYSTEM UPDATE', 'BACKUP', 'RESTORE', and 'CONFIGURATION'. The 'SYSTEM UPDATE' tab is active, showing 'Available updates' (No update available), a 'Check for new updates' button, and a 'System update' section. The 'Advanced properties' section shows the 'Action' as 'Download the firmware update and install it', which is highlighted with a red box. Below this, it shows the 'Current version of the system' as 4.3.6 and 'Update uploaded on this firewall' as 'No updates have been loaded on this firewall'.

The diagram illustrates the update process. On the left, a 'Fichier .maj' (update file) labeled 'Système x+1' is shown. Below it, two partitions are depicted: 'Partition active' containing 'Système x' and 'Config y', and 'Partition passive' containing 'Système x-1' and 'Config y-1'. A large blue arrow points to the right, labeled 'Mise à jour système avec sauvegarde' (system update with backup). On the right, the 'Partition active' now contains 'Système x+1' and 'Config y', while the 'Partition passive' remains 'Système x' and 'Config y'.

STORMSHIELD

27

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

The screenshot displays the 'MAINTENANCE : ACTIVE UPDATE' section of the Stormshield management interface. It features a table of modules and their update status, and a modal window for configuring update servers.

Status	Module
Enabled	Antispam DNS blacklist (RBL)
Enabled	IPS: contextual protection signatures
Disabled	IPS: custom contextual protection signatures
Enabled	Antivirus: ClamAV antivirus signatures
Enabled	Embedded URL databases
Enabled	Antispam: heuristic engine
Enabled	Vulnerability Manager
Enabled	Root Certification Authorities
Enabled	Geolocation / Public IP reputation

**UPDATE SERVERS OF THE URL DATABASE**

URL
https://update1-sns.stormshieldocs.eu/1
https://update2-sns.stormshieldocs.eu/1
https://update3-sns.stormshieldocs.eu/1
https://update4-sns.stormshieldocs.eu/1

**UPDATE SERVERS OF CUSTOM CONTEXTUAL PROTECTION SIGNATURES**

URL	CA
https://update1-sns.stormshieldocs.eu/1	CloudServicesBundle
https://update2-sns.stormshieldocs.eu/1	CloudServicesBundle
https://update3-sns.stormshieldocs.eu/1	CloudServicesBundle
https://update4-sns.stormshieldocs.eu/1	CloudServicesBundle
https://custom-update.mylab.in	Select a CA for HTTPS URLs

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

- o Antispam : listes noires DNS (RBL),
- o Bases d'URLs embarquées,
- o IPS : Signatures de protection contextuelles,

- Antivirus : signatures Antivirales ClamAV (ou antivirus avancé),
  - 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'administration peut modifier, ajouter ou supprimer des serveurs.