

## Fiche Pratique N°30 : Mettez à jour votre box et votre routeur – Sécurisez la porte d'entrée de votre réseau V1.0

**Objectif :** Mettre à jour et sécuriser votre box Internet (ou routeur) pour protéger l'ensemble de vos appareils contre les intrusions, les malwares et les failles de sécurité connues.

**Public visé :** Débutant à Intermédiaire

**Temps estimé :** 15 à 30 minutes

**Niveau de difficulté :** ★★☆☆☆ (Facile – il suffit de se connecter à l'interface de votre box)

**Prérequis :** Un accès à votre box (mot de passe administrateur). Une connexion Internet (évidemment).

### 1. Pourquoi mettre à jour sa box ? (Le problème)

Problème	Explication
<b>La box est la porte d'entrée de votre réseau</b>	Votre box (ou routeur) est le premier point de contact entre Internet et tous vos appareils (ordinateurs, téléphones, TV, imprimantes, objets connectés). Si elle est compromise, tout votre réseau l'est.
<b>Les box sont rarement mises à jour automatiquement</b>	Contrairement à Windows ou Android, les box ne se mettent pas toujours à jour toutes seules (sauf les plus récentes). Des vulnérabilités connues peuvent rester non corrigées pendant des mois, voire des années.
<b>Failles célèbres</b>	Des failles comme <b>VPNFilter</b> (2018, 500 000 routeurs infectés), <b>Mirai</b> (botnet de caméras et routeurs), ou les vulnérabilités DNS ont permis à des pirates de prendre le contrôle de milliers de box.

## Fiche Pratique N°30 : Mettez à jour votre box et votre routeur – Sécurisez la porte d'entrée de votre réseau V1.0

Problème	Explication
<b>Mots de passe par défaut</b>	La plupart des box ont un mot de passe administrateur par défaut (inscrit sous la box). Si vous ne l'avez pas changé, n'importe qui sur votre réseau (ou via une faille) peut prendre le contrôle.
<b>Télémétrie et backdoors</b>	Certains FAI (Fournisseurs d'Accès Internet) collectent des données via votre box. Une box non sécurisée peut aussi être utilisée comme relais pour des attaques (botnet).

**Le bénéfice :** Une box à jour et correctement configurée vous protège contre les attaques extérieures, réduit les risques de piratage de vos appareils, et améliore parfois les performances réseau.

### 2. De quoi parle-t-on ? Box vs routeur

Terme	Explication
<b>Box (Livebox, Freebox, Bbox, SFR Box)</b>	L'appareil fourni par votre FAI (Orange, Free, Bouygues, SFR). Il combine routeur, modem, switch, WiFi et parfois TV/téléphone.
<b>Routeur (personnel)</b>	Appareil que vous avez acheté séparément (ex: Netgear, TP-Link, Asus, Ubiquiti) pour améliorer le WiFi ou ajouter des fonctionnalités.
<b>Passerelle</b>	Terme technique désignant l'appareil qui fait la liaison entre votre réseau local et Internet (votre box, généralement).

**Cette fiche couvre à la fois les box des FAI et les routeurs personnels** (les principes sont les mêmes).

## Fiche Pratique N°30 : Mettez à jour votre box et votre routeur – Sécurisez la porte d'entrée de votre réseau V1.0

### 3. Comment faire ? (Pas à pas)

#### Étape 1 : Trouvez l'adresse IP de votre box

La plupart des box utilisent l'une de ces adresses :

FAI / Routeur	Adresse IP par défaut	Identifiant / Mot de passe (par défaut)
Orange (Livebox)	192.168.1.1	admin / admin (ou mot de passe sous la box)
Free (Freebox)	192.168.1.1 ou mafreebox.freebox.fr	admin / (mot de passe créé à l'installation)
Bouygues (Bbox)	192.168.1.1 ou 192.168.0.1	admin / admin
SFR (SFR Box)	192.168.1.1 ou 192.168.0.1	admin / (mot de passe sous la box)
Routeurs génériques	192.168.1.1, 192.168.0.1, 10.0.0.1	admin / admin (ou password)

#### Méthode pour trouver l'adresse IP :

- Windows** : Ouvrez l'invite de commandes (cmd) → tapez `ipconfig` → regardez la ligne "**Passerelle par défaut**" (Default Gateway).
- Linux / macOS** : Ouvrez un terminal → tapez `ip route | grep default` → l'adresse après `via`.

#### Étape 2 : Connectez-vous à l'interface d'administration

1. Ouvrez votre navigateur (Firefox, Brave, etc.).
2. Tapez l'adresse IP de votre box (ex: 192.168.1.1).
3. Entrez les identifiants (admin / mot de passe).

#### Si vous ne connaissez pas le mot de passe :

- Regardez l'étiquette sous votre box (souvent collée en dessous).

## Fiche Pratique N°30 : Mettez à jour votre box et votre routeur – Sécurisez la porte d'entrée de votre réseau V1.0

• Si vous l'avez changé et oublié : il faut **réinitialiser** la box (petit trou "Reset" à maintenir enfoncé 10-30 secondes). Vous perdrez vos configurations (WiFi, mots de passe, etc.) – à faire en dernier recours.

### Étape 3 : Vérifiez et appliquez les mises à jour

#### Livebox (Orange) :

- Connectez-vous à l'interface → "**Paramètres avancés**" → "**Mise à jour**" (ou "Maintenance").
- Cliquez sur "**Rechercher une mise à jour**".
- Si une mise à jour est disponible, appliquez-la. La box redémarre.

#### Freebox :

- Interface [mafreebox.freebox.fr](http://mafreebox.freebox.fr) → "**Paramètres**" → "**Mise à jour**".
- Free met généralement à jour automatiquement, mais vérifiez.

#### Bbox (Bouygues) :


- Interface → "**Paramètres**" → "**Maintenance**" → "**Mise à jour**".

#### SFR Box :

- Interface → "**Administration**" → "**Mise à jour**".

#### Routeur personnel (TP-Link, Netgear, Asus, etc.) :

- Interface → "**System**" ou "**Firmware Update**" → cliquez sur "Check" ou "Rechercher".
- Téléchargez le firmware sur le site du fabricant (si l'auto-recherche ne fonctionne pas) puis importez-le.

 **Important** : Une mise à jour de firmware prend quelques minutes. **Ne coupez pas l'alimentation** pendant la mise à jour, sinon votre box peut être définitivement cassée (RIP).

## Fiche Pratique N°30 : Mettez à jour votre box et votre routeur – Sécurisez la porte d'entrée de votre réseau V1.0

### Étape 4 : Changez le mot de passe administrateur par défaut

**Pourquoi ?** Si vous gardez `admin / admin`, n'importe quel logiciel malveillant sur votre réseau (ou une faille) peut prendre le contrôle de votre box.

1. Dans l'interface, cherchez "**Administration**" → "**Mot de passe**".
2. Changez le mot de passe administrateur par un mot de passe **fort** (12-16 caractères, mix lettres/chiffres/symboles). Stockez-le dans Bitwarden (fiche N°16).
3. **Ne perdez pas ce mot de passe.**

### Étape 5 : Désactivez l'accès à l'interface depuis Internet

**Pourquoi ?** Pour empêcher un pirate de l'extérieur de tenter de se connecter à votre box.

- Cherchez "**Accès distant**" (Remote Management, WAN Access, Management from Internet).
- **Désactivez** cette option (doit être sur "Désactivé" ou "Local network only").
- (Sauf si vous avez besoin d'y accéder depuis l'extérieur – cas très avancé).

### Étape 6 : Désactivez UPnP (Universal Plug and Play)

**Pourquoi ?** UPnP permet aux appareils de votre réseau d'ouvrir automatiquement des ports sur votre box. C'est pratique pour les jeux vidéo ou certaines applications, mais **très dangereux** : un malware peut ouvrir des ports sans votre consentement.

1. Cherchez "**UPnP**" (Universal Plug and Play) dans l'interface.
2. **Désactivez-le** (mettez sur "Désactivé" ou "Non").

**Effet secondaire** : Certains jeux vidéo ou applications (ex: Xbox, PlayStation) peuvent nécessiter une configuration manuelle des ports (redirection). La plupart fonctionnent sans UPnP. En cas de problème, vous pourrez réactiver temporairement ou configurer une redirection manuelle.

## Fiche Pratique N°30 : Mettez à jour votre box et votre routeur – Sécurisez la porte d'entrée de votre réseau V1.0

### Étape 7 : Désactivez le WiFi WPS (Wi-Fi Protected Setup)

**Pourquoi ?** WPS (bouton physique sur la box) permet de connecter facilement un appareil au WiFi. Mais il existe des failles permettant de casser le code PIN WPS en quelques heures. **Désactivez-le.**

1. Cherchez **"WPS"** (ou "Configuration sécurisée WiFi").
2. Désactivez-le (sur "Désactivé").

### Étape 8 : Configurez le WiFi sécurisé

Paramètre	Valeur recommandée	Pourquoi
<b>Nom du réseau (SSID)</b>	Ne révélez pas votre identité (évitez Freebox-123 ou Livebox-5678). Choisissez un nom neutre (ex: CafeWifi, Bunker, ou le nom par défaut).	Réduit les risques d'attaque ciblée.
<b>Chiffrement</b>	<b>WPA2-AES</b> (ou <b>WPA3</b> si disponible)	Évitez WPA (cassé) ou WEP (très faible).
<b>Mot de passe WiFi</b>	Mot de passe fort (12+ caractères, mix lettres/chiffres/symboles)	Empêche les voisins ou passants de se connecter (et d'attaquer votre réseau).
<b>Masquage du SSID</b> (optionnel)	Peut être activé (le réseau WiFi n'apparaît pas dans la liste, il faut entrer le nom manuellement)	Sécurité par l'obscurité : simple, mais pas une protection absolue.

### Étape 9 (optionnel) : Changez les serveurs DNS

**Pourquoi ?** Le DNS par défaut de votre FAI peut collecter vos données et est souvent moins sécurisé.

## Fiche Pratique N°30 : Mettez à jour votre box et votre routeur – Sécurisez la porte d'entrée de votre réseau V1.0

• Voir la **fiche N°6** (Changez votre serveur DNS) – les réglages se font parfois sur la box (recommandé pour tout le réseau).

### Étape 10 (optionnel) : Désactivez le "port 25" (SMTP) si inutilisé

**Pourquoi ?** Le port 25 (email sortant) peut être utilisé par des malwares pour envoyer des spams depuis votre réseau.

- Dans l'interface, cherchez "**Redirection de ports**" ou "**NAT**".
- Si vous ne faites pas tourner de serveur email, assurez-vous que le port 25 n'est pas redirigé vers un appareil.

### 4. Tableau récapitulatif des actions de sécurisation

Action	Où la trouver	Pourquoi	Priorité
<b>Mettre à jour le firmware</b>	Maintenance / Mise à jour	Corriger les failles connues	<b>Haute</b>
<b>Changer mot de passe admin</b>	Administration / Compte	Empêcher la prise de contrôle	<b>Haute</b>
<b>Désactiver accès distant (WAN)</b>	Administration / Accès distant	Empêcher les attaques externes	<b>Haute</b>
<b>Désactiver UPnP</b>	Avancé / UPnP	Éviter l'ouverture de ports malveillants	<b>Haute</b>
<b>Désactiver WPS</b>	WiFi / WPS	Éviter le cassage du PIN	<b>Haute</b>
<b>Configurer WiFi (WPA2/WPA3)</b>	WiFi / Sécurité	Protéger votre réseau local	<b>Haute</b>
<b>Changer mot de passe WiFi</b>	WiFi	Empêcher les connexions indésirables	<b>Haute</b>
<b>Changer DNS</b>	Réseau / DNS (voir fiche N°6)	Confidentialité, sécurité	Moyenne

## Fiche Pratique N°30 : Mettez à jour votre box et votre routeur – Sécurisez la porte d'entrée de votre réseau V1.0

Action	Où la trouver	Pourquoi	Priorité
Désactiver port 25	Redirection de ports / NAT	Éviter l'envoi de spams	Basse

### 5. À savoir avant de se lancer

Crainte fréquente	La réalité
"Je risque de casser ma box si je fais une mauvaise manipulation."	Très peu de risques. Les interfaces sont prévues pour les non-experts. Ne touchez pas à des paramètres obscurs (VLAN, MTU, etc.) si vous ne savez pas ce qu'ils font.
"Les mises à jour de box, c'est automatique, non ?"	Pas toujours. Certains FAI mettent à jour automatiquement (Free, Orange récemment), d'autres non (SFR a eu des soucis). Vérifiez manuellement au moins une fois par an.
"Je n'arrive pas à me connecter à ma box (mot de passe oublié)."	Il faut réinitialiser la box (petit trou "Reset" à maintenir 10-30 secondes). Attention : vous perdrez votre configuration WiFi (nom, mot de passe) et devrez la reconfigurer.
"UPnP, c'est pratique pour mes jeux (Xbox, PlayStation)."	UPnP ouvre des ports automatiquement. Mais des malwares peuvent l'utiliser. Préférez une redirection manuelle (port forwarding) pour vos jeux, ou réactivez UPnP uniquement le temps du jeu (puis désactivez).
"Mon FAI peut-il voir que j'ai changé mon DNS ?"	Oui, mais ce n'est pas un problème. Le DNS modifié n'affecte que la résolution des noms, pas la connexion Internet.
"Dois-je faire ça sur ma box ET sur mon routeur personnel ?"	Si vous avez un routeur personnel connecté à votre box, vous devez sécuriser les deux. La box reste la passerelle, mais le routeur gère votre réseau local.

## Fiche Pratique N°30 : Mettez à jour votre box et votre routeur – Sécurisez la porte d'entrée de votre réseau V1.0

### 6. Plan d'action par fréquence

Fréquence	Action
Tous les 3-6 mois	Vérifier les mises à jour du firmware (box et routeur).
Tous les 6-12 mois	Vérifier le mot de passe administrateur (toujours fort ?) et le mot de passe WiFi.
Occasionnellement	Vérifier les redirections de ports actives (NAT) – y a-t-il des règles inattendues ?
Si vous quittez votre domicile longtemps	Éteignez la box (ou sécurisez-la). Les box éteintes ne peuvent pas être piratées.

### 7. Mise à jour : cas particuliers par FAI

FAI	Mise à jour	Accès à l'interface	Mot de passe admin par défaut
Orange (Livebox)	Automatique la nuit. Vérifiable manuellement depuis 192.168.1.1	192.168.1.1	admin + mot de passe (sous la box)
Free	Automatique (via Freebox OS). Vérifiable depuis mafreebox.freebox.fr	mafreebox.freebox.fr	Créé à l'installation (pas de défaut)
Bouygues (Bbox)	Automatique la nuit. Parfois manuelle via l'interface.	192.168.1.1	admin / admin (ou sous la box)
SFR	Parfois automatique (mais pas toujours fiable). Vérifiez manuellement.	192.168.1.1 ou 192.168.0.1	Sous la box (papier ou étiquette)

## Fiche Pratique N°30 : Mettez à jour votre box et votre routeur – Sécurisez la porte d'entrée de votre réseau V1.0

### 8. Challenge 7 jours

**Challenge** : Pendant 7 jours, mettez en place l'ensemble des mesures de sécurité sur votre box (ou routeur).

**Jour 1** : Trouvez l'adresse IP de votre box. Connectez-vous à l'interface.

**Jour 2** : Vérifiez et appliquez les mises à jour (firmware).

**Jour 3** : Changez le mot de passe administrateur (stockez-le dans Bitwarden).

**Jour 4** : Désactivez l'accès distant (WAN) et UPnP.

**Jour 5** : Désactivez WPS. Configurez le WiFi en WPA2/WPA3, changez le mot de passe.

**Jour 6** (optionnel) : Changez les DNS (voir fiche N°6).

**Jour 7** : Redémarrez la box (coupez l'alimentation 10 secondes). Vérifiez que tout fonctionne (Internet, WiFi, etc.).

**À la fin** : Votre box est beaucoup plus sécurisée que la moyenne.

### 9. En résumé (ce que vous gagnez)

Action	Bénéfice
Mettre à jour le firmware	Correction des failles de sécurité connues
Changer mot de passe admin	Empêche la prise de contrôle de votre box
Désactiver accès distant	Bloque les attaques depuis Internet

## Fiche Pratique N°30 : Mettez à jour votre box et votre routeur – Sécurisez la porte d'entrée de votre réseau V1.0

Action	Bénéfice
Désactiver UPnP	Empêche l'ouverture de ports par des malwares
Désactiver WPS	Évite le cassage du code PIN WiFi
Configurer WiFi (WPA2/WPA3)	Protège votre réseau local
Changer mot de passe WiFi	Empêche les connexions indésirables

### Conclusion générale

Si vous êtes...	Priorité
Un particulier avec une box FAI (Orange, Free, etc.)	Changez le mot de passe admin, désactivez UPnP et WPS, mettez à jour le firmware.
Un utilisateur avec un routeur personnel	Idem, plus accès à des fonctionnalités avancées (logs, VPN, pare-feu).
Une entreprise / association	Suivez ces recommandations + désactivez les services inutiles, activez les logs, changez le mot de passe régulièrement.

#### À retenir absolument :

- **Votre box est la porte d'entrée de votre maison numérique.** Négliger sa sécurité, c'est inviter les pirates chez vous.
- **Les trois actions les plus importantes** : (1) mettre à jour le firmware, (2) changer le mot de passe administrateur, (3) désactiver UPnP.
- **Les mises à jour ne sont pas toujours automatiques** : vérifiez manuellement au moins une fois par an.
- **Notez vos mots de passe** (admin, WiFi) dans Bitwarden (fiche N°16). Ne les perdez pas.

### Test final :

1.Connectez-vous à votre box (IP : 192.168.1.1).

## Fiche Pratique N°30 : Mettez à jour votre box et votre routeur – Sécurisez la porte d'entrée de votre réseau V1.0

- 2.Vérifiez la version du firmware (date). Comparez avec la dernière version disponible sur le site de votre FAI.
- 3.Changez le mot de passe administrateur (mettez un mot de passe fort).
- 4.Désactivez UPnP (trouvez l'option – faites une recherche dans l'interface si nécessaire).
- 5.Désactivez WPS (trouvez l'option).
- 6.Redémarrez la box.
- 7.Vérifiez que vous pouvez toujours vous connecter à l'interface (avec le nouveau mot de passe).
- 8.Vérifiez que votre WiFi fonctionne toujours (si vous avez changé le mot de passe WiFi, reconnectez vos appareils).
- 9.Si tout fonctionne : **votre box est sécurisée** 