



# GUIDE – SECURISEZ VOS RESEAUX SANS FIL

TRUCS ET ASTUCES SUR COMMENT PROTEGER VOTRE  
RESEAU PERSONNEL DES INTRUSIONS

**BOGDAN BOTEZATU**  
EQUIPE DE COMMUNICATION ET D'ANALYSE DES E-MENACES

PARTICULIERS

 **bitdefender**

## Table des matières

Table des matières.....	2
<i>Pourquoi des réseaux sans fil au lieu de réseaux câblés ?.....</i>	<i>3</i>
<i>Que faire pour un maximum de sécurité ? .....</i>	<i>4</i>
Accès administratif à distance.....	4
Cryptage du trafic sans fil.....	5
Paramétrage des politiques d'accès MAC (Media Access Control) .....	6
Ne pas diffuser le SSID.....	7
Diminuer la portée de la transmission.....	8
<i>Les risques d'utiliser des réseaux non sécurisés ou de s'y connecter .....</i>	<i>9</i>
<i>Conseils de sécurité concernant les bornes d'accès .....</i>	<i>11</i>
<i>Comment BitDefender peut-il vous aider ? .....</i>	<i>12</i>

## Pourquoi des réseaux sans fil au lieu de réseaux câblés ?

Les radiocommunications sont le meilleur moyen de couvrir des zones importantes sans avoir à investir dans le câblage, à effectuer des travaux dans les bâtiments ou à éliminer les encombrements. Cependant, elles constituent un défi constant pour la sécurité, dans la mesure où les informations circulent librement sous la forme d'ondes radio et sont accessibles à tous dans la zone de leur portée, bien qu'elles soient souvent cryptées.

Ce manuel vous indiquera les meilleures pratiques à adopter pour utiliser les réseaux sans fil, et aussi la façon de sécuriser votre propre routeur ou point d'accès pour empêcher d'autres personnes de s'introduire dans votre réseau.

Parmi les avantages les plus évidents d'utiliser un réseau sans fil 802.11 b / g / n chez soi ou dans une petite structure professionnelle, on peut citer le faible coût de l'équipement (point d'accès ou routeur et cartes réseau sans fil), le fait qu'il n'est pas envahissant (inutile de percer les murs ou de tirer des câbles), et la grande liberté d'action qu'il procure. La présence d'un adaptateur sans fil sur les ordinateurs portables, les netbooks et certains téléphones mobiles, a également contribué à l'adoption des communications sans fil.

En dépit du fait que les informations entre le client et le point d'accès ou le routeur circulent librement et sont accessibles par n'importe quel autre client dans la zone de portée, un réseau sans fil bien configuré est totalement protégé.

## Que faire pour un maximum de sécurité ?

Par défaut, les routeurs et les bornes d'accès quittent l'usine avec peu ou pas du tout de protection. La plupart des routeurs et des points d'accès comportent **une zone d'administration**, disponible en accédant à l'adresse IP du matériel par l'intermédiaire d'un navigateur. Dans cette zone, il est demandé d'indiquer un nom d'utilisateur et un mot de passe paramétrés par le fabricant, généralement propres à chaque modèle, et consultables par n'importe qui sur Internet.

### Accès administratif à distance

La plupart des matériels sans fil peuvent en fait fonctionner dès leur déballage grâce à toutes les technologies et fonctionnalités élaborées pour faciliter leur utilisation y compris par des consommateurs non techniquement avertis. L'erreur la plus courante commise par les utilisateurs est de laisser l'appareil « tel qu'il était dans la boîte » puisqu'il fonctionne de toute façon. Il est absolument nécessaire de changer le mot de passe dès que le matériel a été branché et activé.

Sécuriser la console d'administration va empêcher qu'une personne non autorisée puisse modifier vos paramètres réseau et/ou effectuer des opérations telles que l'effacement des données d'accès, afin de rester invisible pendant qu'elle est connectée à d'autres réseaux.

Pour mieux limiter les intrusions dans la zone d'administration, il est également préférable de désactiver l'accès à distance du périphérique sans fil. La plupart des routeurs et des points d'accès permettent à un utilisateur autorisé de modifier la configuration du matériel, même s'il ne se trouve pas sur place – simplement en entrant dans un navigateur son adresse IP.

Cette possibilité se révèle particulièrement utile pour les administrateurs système qui doivent localiser un problème tard dans la nuit, car elle leur permet de le faire à partir de chez eux, mais le routeur se trouve ainsi exposé à toute personne essayant d'obtenir l'adresse IP associée à l'interface publique du périphérique.

Si le routeur n'accepte pas le paramétrage d'une liste d'adresses IP autorisées<sup>1</sup> à accéder à la zone d'administration, il est judicieux d'éteindre l'interface d'administration à distance.

## Cryptage du trafic sans fil

En dehors de la sécurisation de la zone d'administration d'un périphérique sans fil, il est indispensable d'accorder une attention particulière à la connexion elle-même. Nous avons signalé plus haut dans ce document que, en dehors des infrastructures d'un réseau câblé, qui véhiculent les signaux entre routeur et ordinateur - un réseau par défaut digne de confiance - un signal sans fil se propage largement, dans des limites qui ne dépendent que de la puissance de transmission. En fonction de la zone couverte, des dizaines d'ordinateurs peuvent essayer sans autorisation de se connecter à votre réseau, voire, ce qui est pire, pénétrer dans le flot d'informations qui circulent sans avoir été cryptées.

C'est pourquoi il est essentiel que le propriétaire d'un routeur sans fil paramètre une ligne de défense solide en cryptant la connexion avec un code *pre-shared key* (PSK). Pour maintenir des prix bas et diminuer la difficulté du déploiement, les équipements sans fil destinés aux particuliers sont généralement livrés avec deux protocoles de cryptage, à savoir Wired Equivalent Privacy (WEP) et Wi-Fi Protected Access (WPA / WPA2).

Security	
This page allows you setup the wireless security. Turn on WEP or WPA by using Encryption Keys could prevent any unauthorized access to your wireless network.	
Encryption :	WPA pre-shared key ▾
WPA Unicast Cipher Suite :	<input type="radio"/> WPA(TKIP) <input checked="" type="radio"/> WPA2(AES) <input type="radio"/> WPA2 Mixed
Pre-shared Key Format :	Passphrase ▾
Pre-shared Key :	*****
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

*Le protocole WPA2 assure beaucoup plus de protection que le standard de cryptage WEP aujourd'hui critiqué.*

---

<sup>1</sup> Certains routeurs peuvent automatiquement donner accès à la console d'administration uniquement si l'adresse IP est égale à une valeur donnée ou se trouve dans une plage d'adresses IP. Les autres requêtes sont rejetées automatiquement.

**MAC Address Filtering Table**  
It allows to entry 20 sets address only.

NO.	MAC Adress	Comment	Select
1	00:1f:e1:9b:4f:2b	Lori's Dell	<input type="checkbox"/>
2	00:23:4d:c1:5a:62	Bogdan's Dell	<input type="checkbox"/>
3	00:0e:2e:f4:06:0b	Kappa's PC	<input type="checkbox"/>
4	00:24:d6:51:9d:06	Bog's Dell	<input type="checkbox"/>
5	00:21:63:28:c1:39	Cati's Laptop	<input type="checkbox"/>

*Grâce au filtrage par MAC, le routeur n'accepte que les clients de la liste blanche.*

Les deux protocoles utilisent un mode d'authentification sous forme de PSK qui se comportent comme des mots de passe, mais la sécurité n'est pas la même dans les deux cas. WEP est apparu en 1997, intégré dans le protocole 802.11, mais il est maintenant désapprouvé en raison de sérieuses imperfections qui permettent de le déchiffrer facilement. WPA et WPA2 offrent un solide niveau de sécurité tout en ne réclamant qu'un minimum de travail de configuration, ce qui fait d'eux le meilleur choix pour les réseaux sans fil personnels.

Il existe des cas où l'utilisation de WPA est impossible – en particulier lorsque l'infrastructure du réseau a été construite à partir de matériels anciens achetés avant l'introduction des normes. Si votre matériel n'est pas compatible avec WPA, la première démarche est de vérifier auprès du vendeur s'il existe une mise à jour du microprogramme permettant d'intégrer WPA.

Même s'il n'existe aucune mise à jour disponible, vous devriez faute de mieux opter pour WEP plutôt que de laisser votre connexion non cryptée, mais n'oubliez pas que vous exposez vos données à des intrus potentiels et qu'il serait plus avisé de dépenser une trentaine d'euros pour acheter un nouveau routeur déjà compatible avec les protocoles WPA/WPA2.

## Paramétrage des politiques d'accès MAC (Media Access Control)

Une autre méthode de filtrage et d'élimination des intrus est de définir des politiques concernant l'identité des ordinateurs qui tentent de se connecter au réseau sans fil. La plupart des routeurs et des points d'accès SOHO sont compatibles avec le contrôle d'accès MAC, ce qui signifie que le routeur n'acceptera que les connexions en provenance d'une liste de clients pré-définie, clients qui s'identifient avec le MAC de leur périphérique sans fil.

**Wireless Setting**

This page allows you to define ESSID, and Channel for the wireless connection. These parameters are used for the wireless stations to connect to the Access Point.

Mode :	AP
Band :	2.4 GHz (B+G)
ESSID :	Sphynx Soft Romania
Channel Number :	9
Associated Clients :	Show Active Clients

*La diffusion du SSID indique à l'utilisateur qu'il existe un réseau sans fil à proximité.*

Certains périphériques sans fil permettent à l'utilisateur de modifier l'adresse MAC à la demande, ce qui signifie que le filtrage MAC n'est pas à lui seul une solution efficace pour tenir les intrus à distance. C'est cependant une précaution supplémentaire qui, associée à un PSK WPA fiable, augmentera la sécurité de votre réseau sans fil.

Les trois initiatives précédentes constituent les moyens les plus courants de sécuriser un réseau et d'empêcher des utilisateurs non autorisés (par exemple des voisins ou des pirates de WLAN) de s'y connecter. Dans la rubrique qui suit nous allons parler de la façon de dissimuler votre réseau pour le rendre inaccessible aux attaquants qui souhaitent y pénétrer de force.

### Ne pas diffuser le SSID

Pour permettre à l'utilisateur humain de distinguer un réseau sans fil d'un autre, les routeurs et points d'accès diffusent automatiquement leur nom (ESSID / SSID ou Service Set ID). Si la méthode est commode pour le propriétaire du réseau, elle convient également aux attaquants, dans la mesure où le routeur passe son temps à « crier » pour attirer l'attention sur sa présence. Désactiver la diffusion SSID rendra le routeur (comme tous les clients qui lui sont connectés) invisible à ceux qui ignorent qu'il existe un émetteur sans fil dans le secteur.



*La diffusion du SSID indique à l'utilisateur qu'il existe un réseau sans fil à proximité. Les attaquants peuvent exploiter cette diffusion pour leur propre usage.*

## Diminuer la portée de la transmission

Exactement comme n'importe quel appareil radio, le routeur/le point d'accès peut couvrir une zone proportionnelle à la puissance de l'émetteur intégré. La valeur de sortie d'usine est suffisante pour couvrir la surface d'une maison ou celle du trottoir qui la borde, ce qui signifie que tout propriétaire d'un netbook ou d'un ordinateur portable peut tenter d'entrer de force dans votre réseau. Diminuer la portée de transmission permet en général de faire en sorte que le routeur ne transmette pas en dehors de chez vous, ce qui rend sa détection impossible.

Certains routeurs SOHO et points d'accès hauts de gamme possèdent des paramètres qui peuvent diminuer la puissance de transmission de l'adaptateur WLAN. Il n'existe pas de valeur magique pré-calculée susceptible d'offrir le meilleur dosage entre sécurité et performance.

Si vous modifiez la puissance de sortie du WLAN, n'oubliez pas que l'augmentation de la puissance de transmission peut provoquer l'arrivée d'hôtes non invités à la fête, tandis qu'une diminution trop forte de la puissance de transmission peut dramatiquement réduire la performance du réseau en termes de transfert de données.

La puissance de transmission peut être contrôlée, même sur des matériels dont le logiciel interne est dépourvu de cette option. La simple suppression de l'antenne de l'appareil (ou de l'une d'entre elles s'il en possède plusieurs) peut aussi permettre de rendre les signaux suffisamment faibles pour ne pas être interceptés, mais suffisants pour être performants à l'intérieur de la maison.

L'emplacement du routeur est également important. En règle générale, il est déconseillé de placer le routeur sans fil ou le point d'accès près d'une fenêtre donnant sur un espace public, car les ondes radio se propagent mieux à travers une vitre qu'à travers le béton.



*Le pare-feu de BitDefender détecte automatiquement les réseaux non sécurisés et conseille à l'utilisateur de prendre les mesures qui s'imposent.*

## Les risques d'utiliser des réseaux non sécurisés ou de s'y connecter

De manière générale, les réseaux non sécurisés sont des sources de tracas. A quelques exceptions près, quand ils se retournent en fait contre « l'envahisseur », les réseaux non sécurisés sont pour leurs propriétaires à l'origine d'importantes pertes de données.

Les réseaux domestiques sont fondés sur la confiance : aucuns mécanismes coûteux d'authentification ne sont installés pour limiter l'accès à une ressource ou une autre. Au contraire, les utilisateurs à domicile ont tendance à tout rendre disponible, de manière à ce que les informations contenues dans un ordinateur soient accessibles aux autres PC dans la maison.

Les dossiers non protégés de **partage de fichiers sur le réseau**, contenant des données d'ordre personnel (documents et images, par exemple, pour n'en citer que certains) sont un des points faibles les plus courants des réseaux domestiques. Quand des utilisateurs non autorisés se connectent à un réseau non sécurisé, ils peuvent aussi avoir accès aux fichiers partagés, ce qui signifie qu'ils peuvent copier des photos de famille, des documents ou des fichiers multimédia comme des jeux ou des films. Si ces fichiers sont modifiables, l'attaquant peut effacer le contenu du dossier, ou même installer du malware sous l'apparence d'innocents fichiers destinés à être exécutés par l'utilisateur.

Le « **reniflage** » de paquets et l'interception du trafic constituent quelques autres sujets d'inquiétude si un réseau est envahi. Par principe, le trafic réseau circule librement d'un ordinateur à l'autre. C'est l'ordinateur qui détermine quel trafic accepter ou rejeter si les informations ne lui sont pas destinées. Un « membre du réseau » malintentionné peut suivre l'ensemble du trafic avec des outils spécifiques et les utiliser à la recherche d'échanges sur messagerie instantanée, de noms d'utilisateurs et de mots de passe qui n'ont pas été envoyés par SSL, etc.

Le **sidejacking** est une forme de reniflage de paquets, mais qui est beaucoup plus efficace que de suivre bêtement des échanges pour trouver des mots de passe et des noms d'utilisateurs envoyés en clair. Ce type d'attaque intercepte les cookies échangés entre les utilisateurs authentifiés et les sites web correspondants. Cette attaque est efficace même à l'encontre des services web utilisant l'authentification SSL pour crypter le nom d'utilisateur et le mot de passe avant de les envoyer au serveur. Si le cookie tombe entre les mauvaises mains, il peut être utilisé comme moyen d'authentification auprès d'un service web, à l'insu de son propriétaire légitime qui ne sait pas que quelqu'un d'autre utilise son compte.

Les réseaux non sécurisés constituent un terrain idéal pour le déploiement de **tentatives illégales diverses**. En général, les cybercriminels s'attachent à pénétrer les réseaux pour faire des achats en utilisant des cartes de paiement volées, s'introduire dans des espaces privés ou illégalement télécharger de la musique, des films ou des logiciels via P2P, pour masquer leur identité derrière l'adresse IP du réseau non sécurisé. Si la police décide de poursuivre le contrevenant, elle s'attaquera en fait au propriétaire du réseau ouvert. A d'autres moments, les cyberescrocs utilisent les réseaux sans fil non sécurisés pour envoyer d'énormes quantités de spam de la part du propriétaire du réseau, ce qui a pour conséquence des enquêtes supplémentaires, voire la clôture de l'abonnement à Internet.

Se connecter à des réseaux non sécurisés est également dangereux car le trafic circulant entre vous et le routeur ou le point d'accès peut facilement être intercepté par des personnes malintentionnées connectées au même réseau. Vous pouvez également **exposer des dossiers de partage** configurés pour le réseau domestique ou même être infecté par des vers provenant d'autres systèmes sur le réseau.



## Conseils de sécurité concernant les bornes d'accès

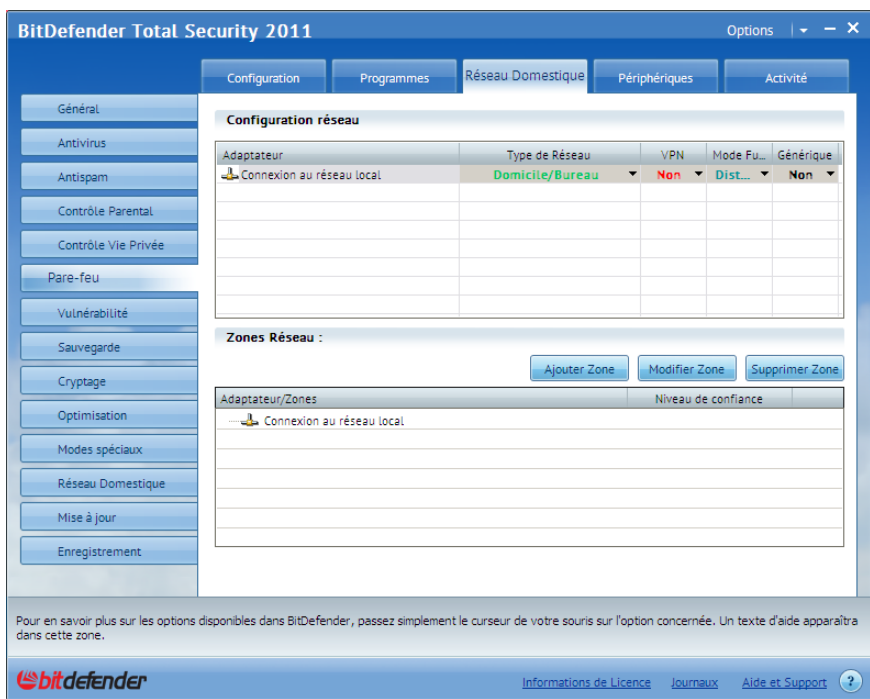
Les bornes d'accès sont assez répandues aujourd'hui, au point que presque tous les jardins publics, les cafés ou les aéroports fournissent un libre accès à Internet à ceux qui ressentent un besoin permanent de se connecter à Internet.

Néanmoins, se connecter à une borne non sécurisée peut engendrer plus d'ennuis que de satisfaction si un minimum de précaution n'est pas pris. Voici quelques conseils destinés à vous aider à rester en sécurité tout en surfant incognito.

Chaque fois que vous vous promenez sur un réseau non sécurisé, pensez au fait que vous ignorez qui sont vos voisins. Ils peuvent tenter de scanner les ports pour détecter les **brèches exploitables** et déjouer la sécurité. Pour minimiser les risques, vous avez intérêt à installer un logiciel pare-feu capable de filtrer les tentatives de connexion à partir des réseaux extérieurs.

Les réseaux publics ne sont pas conçus pour échanger des informations sensibles. Le risque existe qu'un ou plusieurs des utilisateurs partageant la même borne tente de fureter à la recherche d'informations sensibles comme des noms d'utilisateurs, des mots de passe, d'intéressants échanges sur messagerie instantanée ou, encore mieux, des authentifiants bancaires. Il vous est conseillé de prêter la plus grande attention aux services que vous utilisez en vous connectant aux bornes et **dans la mesure du possible d'éviter de le faire**.

Les dossiers partagés constituent un autre aspect dangereux à prendre en compte en se connectant à d'autres réseaux, car vous courez le risque **d'exposer involontairement des données personnelles à la curiosité de personnes non autorisées**. N'oubliez jamais de désactiver les dossiers partagés avant de vous connecter à une borne publique.



*Quand le réseau est de type "public", BitDefender cache automatiquement le PC pour que d'autres ordinateurs sur le réseau ne puissent pas le voir.*

## Comment BitDefender peut-il vous aider ?

BitDefender a présenté en 2001 un module pare-feu, devenant ainsi le premier antivirus au monde possédant un pare-feu intégré. La gamme 2011 des produits BitDefender des familles Internet Security et Total Security possède un pare-feu perfectionné pour répondre aux nécessités qui s'imposent pour des environnements sans fil non sécurisés.

Pour faciliter la configuration, le pare-feu BitDefender propose quatre types de réseau pré-programmés : Confiance, Domicile / Bureau, Public et Non fiable.

Mieux encore, une fois connecté à des réseaux publics, le pare-feu active automatiquement le **Mode furtif** qui va rendre l'ordinateur invisible aux autres systèmes du réseau, ce qui diminue ses risques d'être la cible de malware ou de pirates.

Même quand il n'est utilisé que dans le cadre de votre propre réseau, le pare-feu peut se révéler un bon outil, du fait de l'une de ses caractéristiques qui est d'afficher une notification chaque fois qu'un ordinateur se connecte au réseau.

Ceci est particulièrement utile pour vous aider à vérifier si les ordinateurs qui se connectent appartiennent effectivement à des utilisateurs corrects ou s'il s'agit d'une tentative réussie de piratage.

Les informations et données contenues dans ce document sont la représentation de l'opinion de BitDefender® sur les sujets traités le jour de la publication. Ce document et les informations qui y sont contenues ne doivent pas être interprétés comme un engagement ou un accord de la part de BitDefender.

Même si toutes les précautions ont été prises lors de la rédaction de ce document, l'éditeur, les auteurs et les contributeurs ne pourront être tenu responsables en cas d'erreurs et/ou omissions. Aucune responsabilité ne peut non plus être engagée pour des dommages résultant de l'utilisation d'informations contenues dans ce document. De plus, les informations contenues dans ce document peuvent faire l'objet de corrections, sans annonce préalable. BitDefender, l'éditeur, les auteurs, et les contributeurs ne peuvent garantir la mise à disposition de nouveaux documents ou d'informations supplémentaires en rapport avec ce document-ci.

Ce document et les données contenues dans celui-ci n'ont qu'un but informatif. Si une assistance professionnelle est nécessaire, une personne compétente dans ce domaine devra être contactée. Ni BitDefender, l'éditeur, les auteurs ou les contributeurs ne peuvent être tenus responsables de dommages en résultant.

Le fait qu'un individu ou une organisation, un travail individuel ou collectif (incluant les documents imprimés, les documents électroniques, sites web, etc.) soient cités et/ou soient source d'informations n'implique pas que BitDefender, l'éditeur, les auteurs ou les contributeurs soient responsables des informations ou recommandations que ceux-ci pourraient fournir. Les lecteurs doivent prendre en compte que BitDefender, l'éditeur du document, les auteurs ou les contributeurs ne peuvent garantir la justesse de toute information après la date de publication, comme les adresses web et liens Internet listés dans le document, et qui pourraient avoir changé ou disparu entre le moment où ce document a été rédigé et publié, et le moment où il est lu.

Les lecteurs doivent se conformer aux lois internationales régissant la propriété intellectuelle, concernant toute partie de ce document. Aucune partie de ce document ne peut être reproduite, stockée, ou transmise sous quelque forme ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement, etc.) ou pour toute autre raison, sans la permission écrite de BitDefender.

BitDefender peut avoir breveté des applications, marques, droits d'auteur, ou toute autre propriété intellectuelle couvrant des sujets traités dans ce document. Sauf stipulation expresse dans un contrat de licence écrit de la part de BitDefender, ce document ne donne aucun droit sur les brevets, marques, droits d'auteur ou autre propriété intellectuelle.

Copyright © 2010 BitDefender. Tous droits réservés.

Tous les autres produits et noms d'organisations cités dans ce document le sont à simple but d'identification et sont la propriété et/ou marques de leurs propriétaires respectifs.