SECURING WIRELESS NETWORKS GUIDE

TIPS AND TRICKS ON HOW TO SHIELD YOUR HOME NETWORK FROM INTRUDERS

BOGDAN BOTEZATU
E-THREATS ANALYSIS AND COMMUNICATION TEAM

HOME USERS

bitdefender

Table of Contents

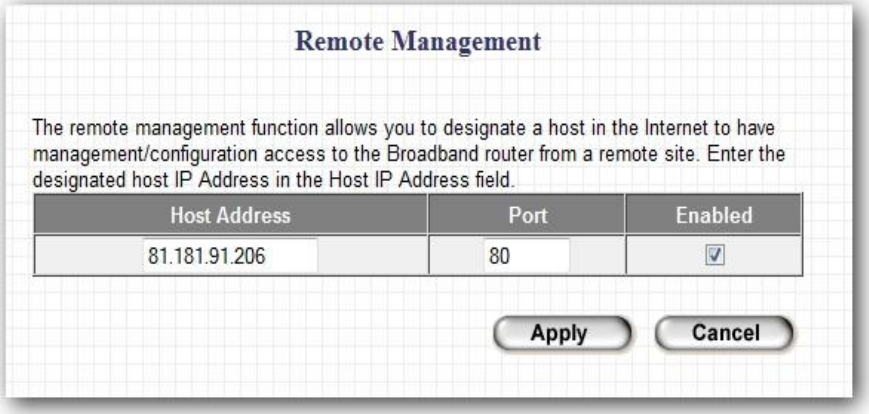
Why wireless over wired networks?

Radio communications are the best way to cover large areas without having to invest in cabling, to perform structural changes when it comes to buildings or to eliminate clutter. However, they have continuously been challenged in terms of security, as information is flowing freely in the form of radio waves and is publicly available to anyone in the coverage area, although it is often encrypted.

The following guide will teach you the best practices when using wireless networking, as well as how to secure your home router or access point to prevent others from abusing your network.

Some of the most obvious advantages of implementing a 802.11 b / g / n wireless network at home or in small offices are the low cost of purchasing wireless hardware (access point or router and wireless network cards), the fact that it is extremely unobtrusive (no need to drill walls or lay out cables), as well as the liberty of movement. The presence of a wireless adapter on laptops, netbooks and some mobile phones has also contributed to the increased adoption of wireless communications.

Despite the fact that the information between the client and the access point or router flows freely and is accessible to any other clients in the coverage area, a well-configured wireless network is completely safe.



Remote management allows you to define which IPs are allowed to see the administrative interface

What exactly needs extra security?

By default, routers and access points leave the factory with little to no security set in place. Most routers and access points feature **a browser-based administrative area** that is available by accessing the device's IP via a browser. Upon accessing it, the device asks for a factory-preset username and password, which is usually typical to each model and publicly available on the Internet.

Administrative access and remote log-ins

Most wireless devices can actually work out-of-the-box thanks to the multitude of technologies and features implemented to facilitate deployment even for non-technical consumers. The most commonly encountered mistake users make is leaving the device "as it was in the box" because it works anyway. It is absolutely mandatory that the password be changed right after the device has been plugged in and powered on.

Securing the administrative backend will prevent an unauthorized individual from tampering with your network settings and / or performing some actions such as flushing access logs, in order to stay stealthy while connected to the others' networks.

In order to further minimize intrusion into the administrative backend, the wireless device's owner should also disable remote access. Most routers and access points allow an authorized user to alter the device's settings - even if they are not in the building - by simply typing into a browser their IP address.

This feature proves to be invaluable for system administrators that have to troubleshoot a connectivity issue late at night, since it allows them to tap in from the comfort of their own home, but it also exposes the router to anyone who tries to access the IP address associated with the device's public interface.

If the router does not accept setting up a list of trusted IP addresses[1] authorized to access the administrative backend, it's advisable to turn off the remote administration interface.

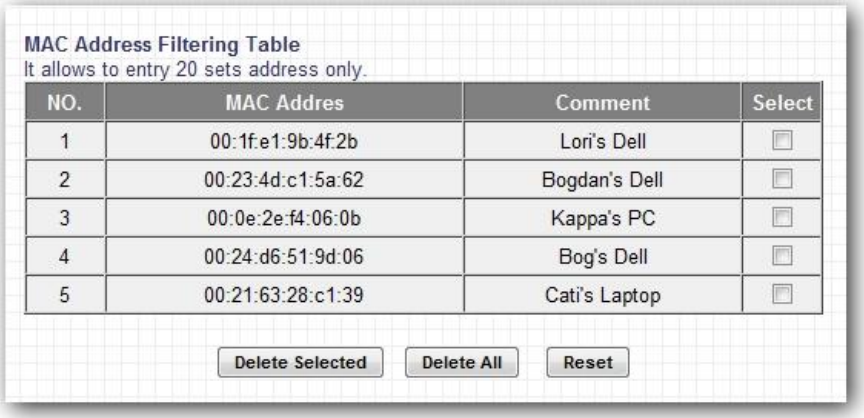
The WPA2 protocol offers much more protection than the deprecated WEP encryption standard

Wireless traffic encryption

Apart from securing the administration area of the wireless device, great attention should be paid to the wireless connection itself. We mentioned earlier in this document that, unlike cabled network infrastructures, which guide signals between the router and a computer – a trustworthy network by default -, wireless signal covers vast spaces, which are only limited by the transmission power. Depending on the coverage area, there may be tens of computers attempting to connect to your network without authorization, or even worse, poke into the stream of information that flows unencrypted.

That is why it is mandatory for the wireless router owner to set up a strong line of defense by encrypting the connection using a pre-shared key. In order to keep pricing down and reduce the complexity of deployment, home wireless devices usually come with two built-in encryption protocols, namely Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA / WPA2).

[1] Some routers can automatically allow access to the administrative console only if the client's IP matches a specific value, or is in a specific IP range. Other requests will be automatically rejected.


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

NO.	MAC Addres	Comment	Select
1	00:1f:e1:9b:4f:2b	Lori's Dell	☐
2	00:23:4d:c1:5a:62	Bogdan's Dell	☐
3	00:0e:2e:f4:06:0b	Kappa's PC	☐
4	00:24:d6:51:9d:06	Bog's Dell	☐
5	00:21:63:28:c1:39	Cati's Laptop	☐

Delete Selected | Delete All | Reset

MAC filtering ensures that the router only accepts clients that have already been whitelisted as trusted.

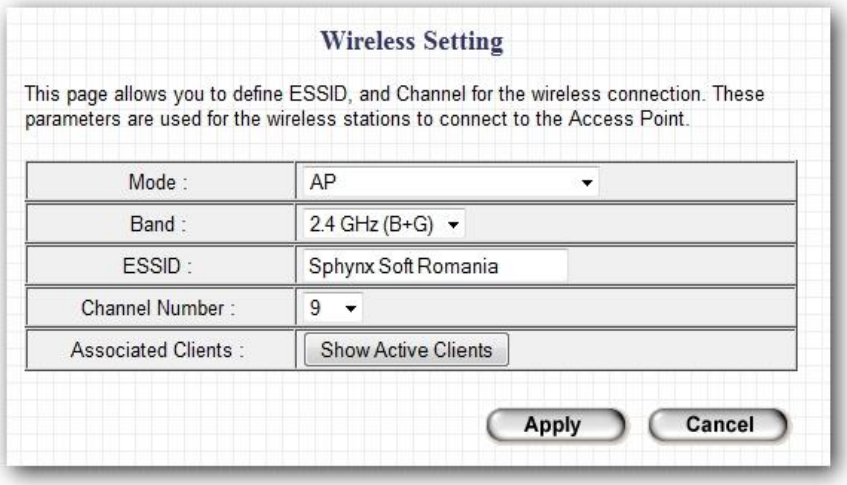
Both protocols rely on a one-factor authentication measure in the form of pre-shared keys that act as passwords, but they are different in terms of security. WEP has been around since 1997, when it was part of the 802.11 protocol, but it has now become deprecated because of some serious flaws that make it easily crack-able. WPA and WPA2 provide a sound level of security while keeping the configuration work to a minimum, which makes them the best pick for home wireless networks.

There are instances when the use of WPA is impossible – mostly when the network infrastructure is built around older hardware that was purchased prior to the introduction of the standard. If your device does not support WPA, the first step to do is check with the vendor if there is any firmware update to include WPA support.

Even if there is no firmware update, you should still choose WEP rather than leaving your connection unencrypted, but please be aware that you are exposing data to a potential intruder and it would be wiser to spend about $30 to buy yourself a new wireless router that supports WPA/WPA2 out of the box.

Setting MAC (Media Access Control) access policies

A secondary method of filtering out the intruders is to define policies regarding the identity of the computer that attempts to connect to the wireless network. Most SOHO routers and access points support MAC-based access control, which means that the router will only accept connections coming from a pre-defined list of clients identifying themselves with their wireless adapter MAC.



SSID broadcasts tell users that there's a wireless network nearby. Attackers may exploit this to their own purpose.

Some wireless adapters allow the user to change the MAC address as needed, which means that MAC filtering alone is not an efficient solution to keep intruders at bay. However, it is an extra precaution that, paired with a strong WPA pre-shared key, will increase your wireless network's security.

The three steps enumerated above are the most common means of securing a network and preventing other unauthorized users (such as neighbors or WLAN hijackers) from connecting to it. In the following section we'll discuss about how to hide your network in order to make it inaccessible to attackers that are willing to force their way through your network.

Stop the SSID broadcast

In order to allow the human user to tell one wireless network from another, routers and access points automatically broadcast their name (also known as ESSID / SSID or Service Set ID). Although convenient for the owner of the network, this method is also convenient for an attacker, as the router would continuously "scream" to draw attention of its presence. Disabling SSID broadcast will make the router (along with all the clients connected to it) invisible to anyone who is not aware that there is an active wireless transmitter in the area.

SSID broadcasts tell users that there's a wireless network nearby. Attackers may exploit this to their own purpose.

Minimize the transmission power

Just like any radio-based device, the router / access point can cover an area that is proportional to the power of the built-in transmitter. The factory-preset value is more than enough to cover a home and even part of the public spaces surrounding it, such as stairways or the sidewalk in front of the house, which means that anyone equipped with a netbook or laptop can attempt to force their way into your network. Minimizing the transmission power actually ensures that the router will not transmit beyond your property, thus making network sniffing impossible.

Some high-end SOHO routers and access points have software settings that can reduce the transmission power of the WLAN adapter. There is no magic pre-computed value to offer the best ratio between security and performance.

When tweaking the WLAN output power, bear in mind that increasing the transmission power can bring you uninvited guests to the WLAN fiesta, while lowering the transmission power too much can dramatically cut down on the network's performance in terms of data transfer.

Transmission power can be controlled even on devices that do not have this option built into the firmware. Simply removing the device's antenna (or one of the antennas, if the wireless device has more than one) will also result in signals low enough to deter interception, but sufficient for high performance inside the house.

The router's physical placement is also affecting coverage. As a rule, never place the wireless router or access point near a window with a view on public places, as radio waves propagate better through glass than through concrete.

The BitDefender Firewall automatically detects unsecured networks and advises the user to take the necessary measures.

Risks of running and connecting to unsecured networks

As a general rule, unsecured networks spell trouble. With a few exceptions when they actually turn against the "invader", unsecured networks are a significant source of data loss for the owner.

Home networks are based on trust: there are no expensive authentication mechanisms set in place to minimize access to one resource or another. On the contrary, home users tend to make everything publicly available, in order for the information from one computer to be accessible to other machines in the household.

Network shares with read and write privileges or holding private information (documents and pictures, for instance, to name only a few) are the most encountered weaknesses in home network. As the unauthorized users successfully connect to an unsecured network, they also gain access to network shares, which means that they can copy family pictures, documents or multimedia files such as games and movies. If these network shares are writable, the attacker may delete the contents of the folder, or even plant malware disguised as innocent files and wait for the user to execute it.

Packet sniffing and traffic interception are some other concerns when it comes to network intrusion. By design, the network traffic flows freely between every computer. It is the computer that chooses which traffic to process and which to discard because the specific information was not destined for it. A misguided "network member" may listen to all the traffic using special tools and process it on the look-out for IM conversations, login details that have not been sent through SSL connections and so on.

Sidejacking is a form of packet sniffing, but it is much more efficient than eavesdropping aimlessly in search of usernames and passwords sent in plain-text. This kind of attack intercepts cookies exchanged between authenticated users and the respective websites. The attack is efficient even against web services that use SSL authentication for encrypting the username and password prior to sending them to the server. Once the cookies fall in the wrong hands, they can be used to authenticate into a web service just like the genuine user, without the latter even knowing that there is someone else using the account.

Unsecured networks are just the right channel for **various illegal purposes**. Usually, cyber-criminals turn to open networks to order products using stolen credit cards, to hack into private spaces or to illegally download music, movies or software via P2P, in order to camouflage their identity behind the IP address of the unsecured network. If the police decide to go after the offender, they will actually end up prosecuting the unwary owner of the open network. Other times, cyber-crooks use unsecured wireless networks to send massive amounts of spam on the network owner's behalf, which will likely result further investigations or even the termination of the Internet subscription.

Connecting to unsecured networks is equally dangerous, as unencrypted traffic flowing between you and the router or access point can be easily sniffed by ill-intended persons connected on the same network. You may also **expose network shares** that have been configured for the home network or even get infected with various worms originating from other systems in the network.

Safety tips while accessing hotspots

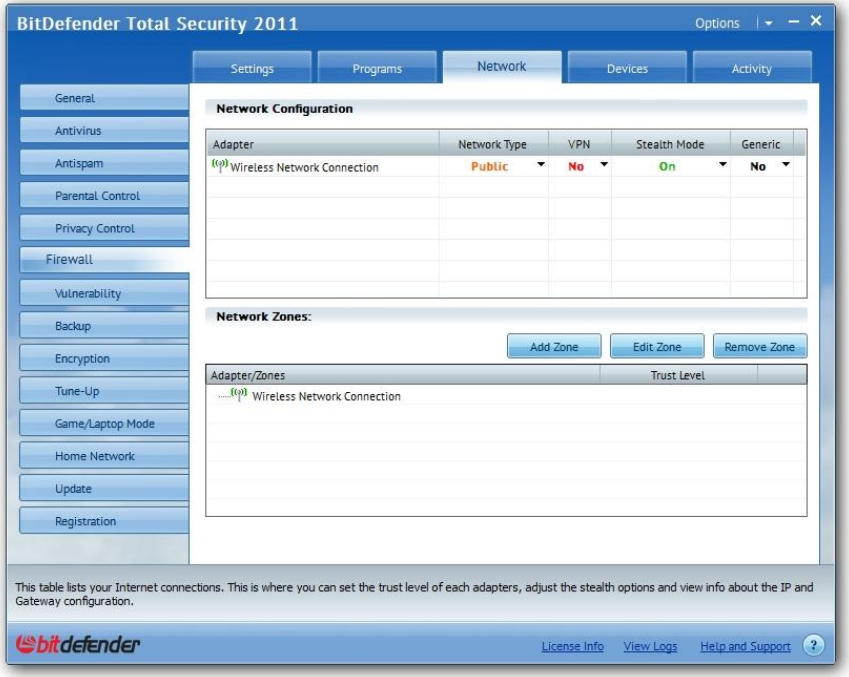
Hotspots are quite common nowadays, so common that almost any park, coffee shop or airport provides free Internet access to those who would like to get in sync with their online reality.

Nevertheless, connecting to an unsecured hotspot may bring more trouble than satisfaction if a minimum level of precaution is not taken. Here are a few guidelines to help you stay safe while surfing incognito.

Whenever roaming in an unsecured network, please remember that you do not know who your neighbors are. They may attempt to run port scans in order to detect **exploitable breaches** and penetrate local security. In order to minimize risks, you should install a firewall application that is able to filter connection attempts from the outside network.

Public networks are not tailored for exchanging sensitive information. Chances are that one or more of the users sharing the same hotspot will try to poke into network traffic coming from and to other computers looking for valuable information such as usernames, passwords, interesting IM conversations or better yet, e-banking authentications. You are advised to pay extra attention to what services you are using while connected to hotspots and **avoid logging in as much as possible**.

Network shares are another critical aspect that needs to be taken into account when connecting to other networks, as you run the risk of unwillingly **exposing private data to unauthorized persons**. Always remember to disable shares before connecting to a hotspot.



BitDefender automatically hides the computer from other clients in the network when the network's profile is set to "Public"

How can BitDefender help you?

BitDefender has introduced the firewall module in 2001, thus becoming the world's first antivirus with a built-in firewall feature. The 2011 series of products in the BitDefender Internet Security and Total Security families feature an improved firewall to meet the security demands in unsecured wireless environments.

In order to facilitate configuration, the BitDefender firewall comes with four pre-set types of network: Trusted, Home / Office, Public and Untrusted.

More than that, when connected to public networks, the firewall automatically activates the **Stealth Mode**, which will automatically hide the computer from other systems in the network, thus minimizing the chances for it to be intercepted by malware or hackers.

Even when used from the comfort of your own network, the firewall may come in just handy, as it has a feature that displays a notification every time a computer connects to the network.

This is particularly important to help you spot whether the systems which are connecting to the network actually belong to legit users or there has been a successful hacking attempt.

bitdefender