

Monitor your child's activity through the Wireless Router

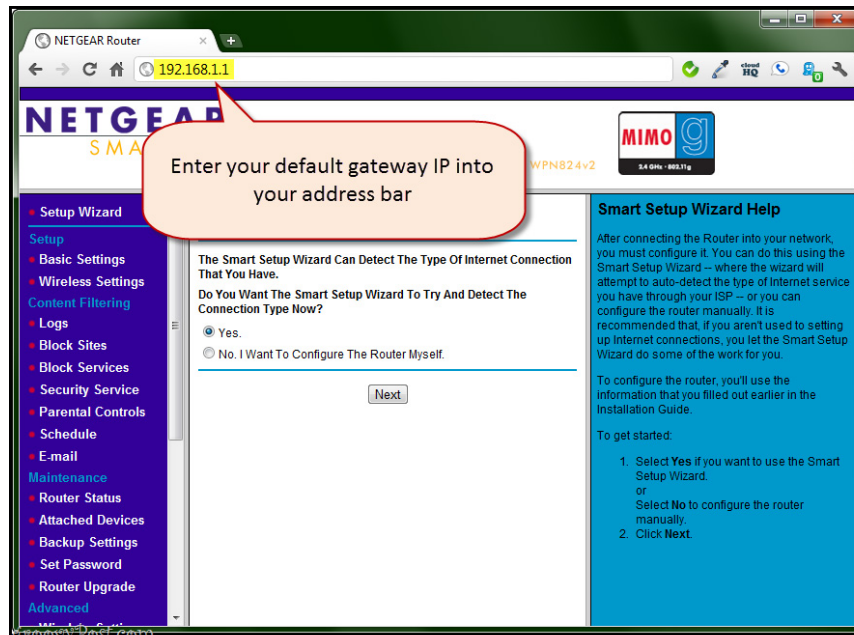
As the world becomes more and more modern with the continuous support of technology and computer science with the current speed, especially the Internet environment, the management, supervision and education of children also become more complex than ever. While parents are trying to create a modern environment ...

TipsMake.com - As the world becomes more and more modern with the continuous support of technology and computer science with the current speed, especially the Internet environment, the management, supervision and education Sex with children also becomes more complex than ever. While parents are trying to create a modern and technological environment to help young children soon contact and apply the advantages that the Internet brings, they do not fully understand the dangers. Danger is lurking here. In the following article, we will show you the specific steps to manage, monitor and record the information flow recorded through the router device (specifically **NETGEAR WPN824v2**) and how to prevent it Block certain websites for computers in your home, without having to install any supporting software on those monitored items.

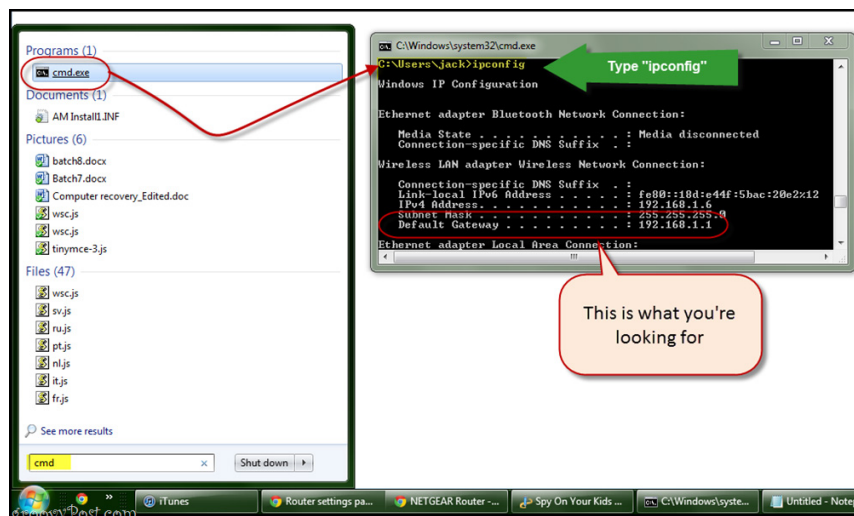
Note that our test is based on **NETGEAR** 's router device, if you are using products from other brands such as **Linksys, Cisco, Belkin or D-Link** , the steps are similar. so.

Visit the router's main control page:

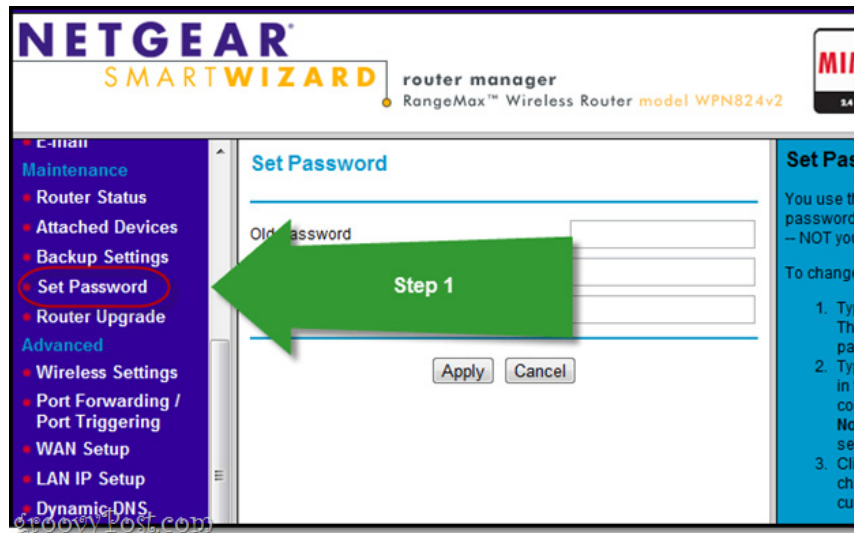
From any computer, please access the main settings and configuration page of the router by typing the IP address into the browser (here is **192.168.1.1**):



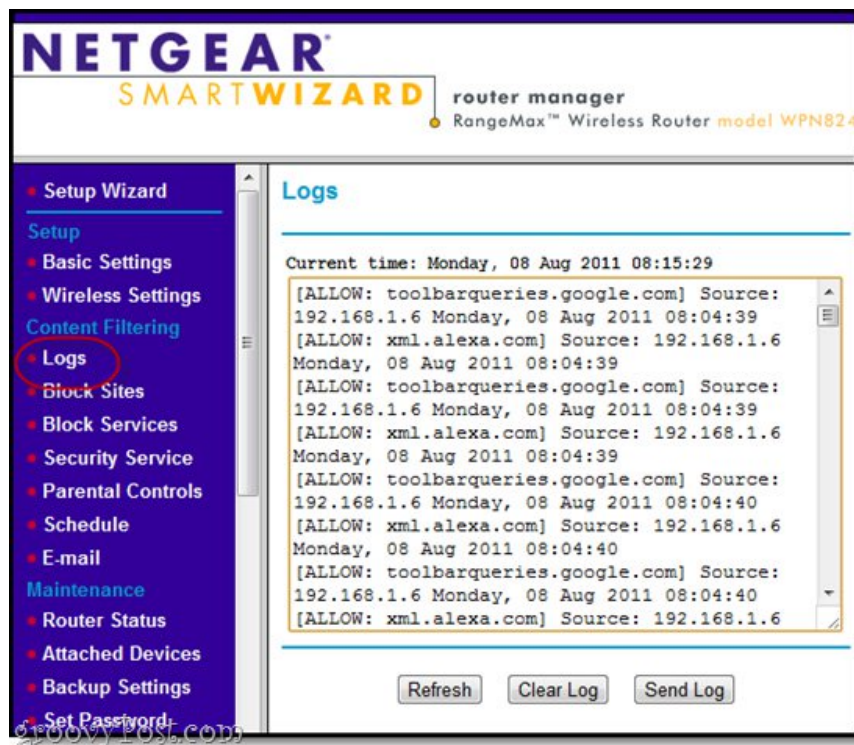
If not, use **Command Prompt (Start Menu> Run> cmd)** and type **ipconfig / all** , then find the **Default gateway** parameter as shown below:



Here, the system will ask you to enter the administrator account information including **Username** and **Password** . The default parameters are mostly **admin - password, admin - 1234, admin - admin or root - root** . If you don't remember, use Google to search the **router model** and the **default password** keyword . After accessing, we should change this account again to avoid risk or others change (if they know and know the default administrator account). With **NETGEAR** , you open **Maintenance> Set Password**:



To get a better idea of ??what we're going to do in the following steps, click **Logs** under **Content Filtering**:



When I look here, most of us won't understand anything, but don't worry, we'll explain it below. If you can analyze and understand all this information, it is too great, if not then continue reading more. At the screenshot above, all we need to note is the IP address and Source section, this is a way to monitor what you want. Specifically, in this test, we will analyze the behavior derived from address **192.168.1.6**.

Check the connected devices:

To do so, select the **Attached Devices** section under **Maintenance** :

NETGEAR
SMARTWIZARD router manager
RangeMax™ Wireless Router model WPN824

Maintenance

- Router Status
- Attached Devices**
- Backup Settings
- Set Password
- Router Upgrade

Advanced

- Wireless Settings
- Port Forwarding / Port Triggering

Attached Devices

| # | IP Address | Device Name | MAC Address |
|---|-------------|----------------|-------------------|
| 1 | 192.168.1.2 | HP8D41B1 | 00:26:55:8d:41:b1 |
| 2 | 192.168.1.4 | PHONEY-BALONEY | 64:b9:e8:03:8f:f3 |
| 3 | 192.168.1.6 | JACK-WIN7 | 00:19:e3:d5:2a:70 |

Refresh

Here, we can see the list of all devices connected via the router. Specifically, **192.168.1.6** is **JACK-WIN7**, which is the name of the computer, while **PHONEY-BALONEY** is a phone, while the **HP8D41B1** is a **netbook** being used somewhere in the house, or it may be a Some "curious" neighbor is accessing our Wifi illegally. To illustrate more clearly, we proceed to access **yahoo.com** on the phone and see what is recorded here:

Attached Devices

| # | IP Address | Device Name | MAC Address |
|---|-------------|----------------|-------------------|
| 1 | 192.168.1.2 | HP8D41B1 | 00:26:55:8d:41:b1 |
| 2 | 192.168.1.4 | PHONEY-BALONEY | 64:b9:e8:03:8f:f3 |
| 3 | 192.168.1.6 | JACK-WIN7 | 00:19:e3:d5:2a:70 |
| 4 | 192.168.1.8 | JACKBUSCH-EEPC | 00:25:d3:8c:1b:53 |

Refresh

Bingo

Logs

Current time: Monday, 08 Aug 2011 08:22:04

```

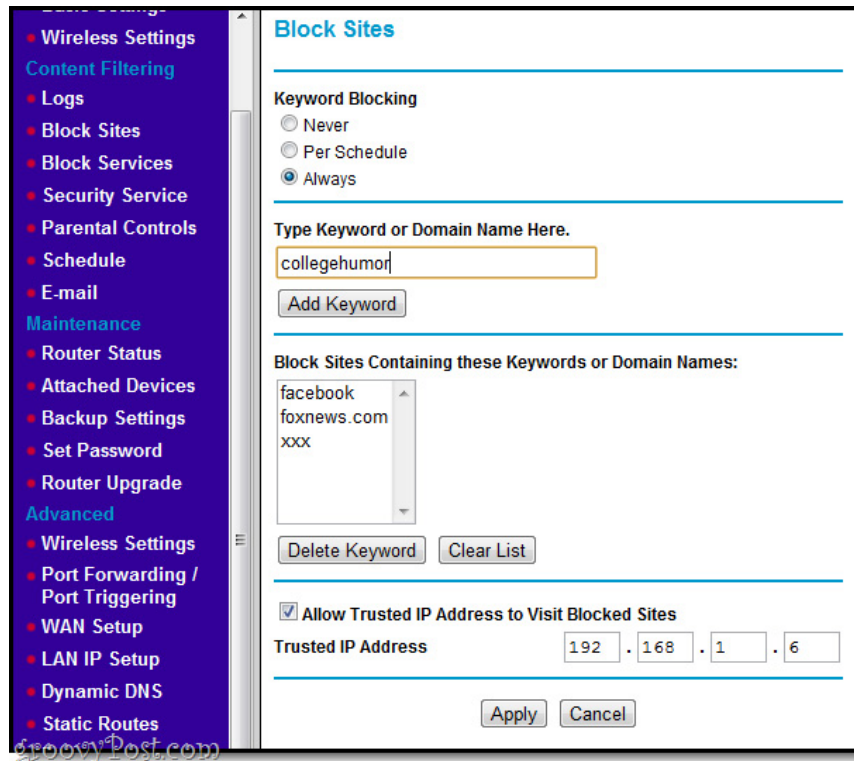
192.168.1.6 Monday, 08 Aug 2011 08:21:45
[ALLOW: xml.alexa.com] Source: 192.168.1.6
Monday, 08 Aug 2011 08:21:46
[ALLOW: toolbarqueries.google.com] Source:
192.168.1.6 Monday, 08 Aug 2011 08:21:51
[ALLOW: xml.alexa.com] Source: 192.168.1.6
Monday, 08 Aug 2011 08:21:51
[ALLOW: toolbarqueries.google.com] Source:
192.168.1.6 Monday, 08 Aug 2011 08:21:51
[ALLOW: xml.alexa.com] Source: 192.168.1.6
Monday, 08 Aug 2011 08:21:51
[ALLOW: m.yahoo.com] Source: 192.168.1.4
Monday, 08 Aug 2011 08:22:02

```

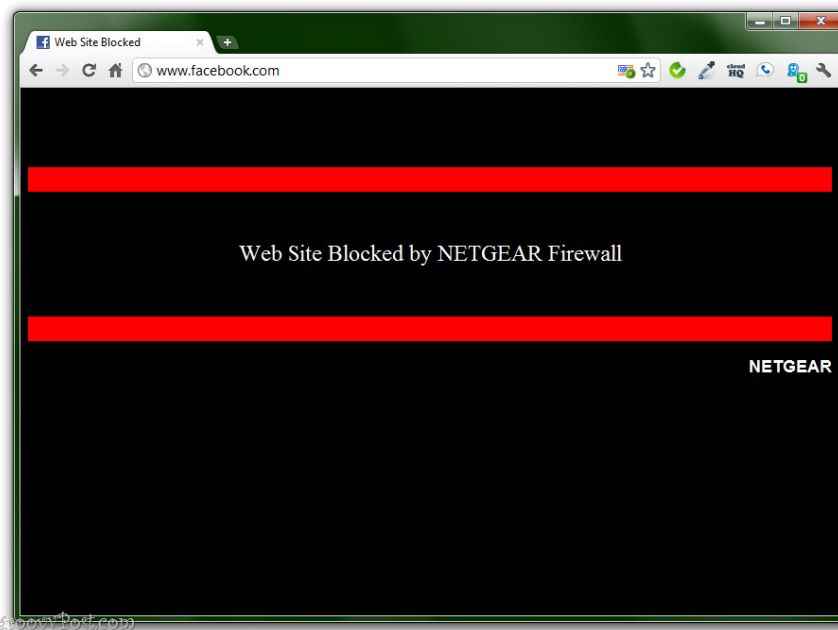
Refresh Clear Log Send Log

However, not everyone has free time to sit and observe this information. Therefore, we can proceed to prevent IP addresses or unwanted websites.

Blocking websites or services on routers is essentially the process of restricting access from certain addresses through specific ports. To do this, you select the **Block Sites** function under **Content Filtering** . Here, we can restrict websites by adding keywords to the Block list, or blocking based on the automatic calendar mode (press **Schedule** to select the time interval by hour, day, week) or full block:

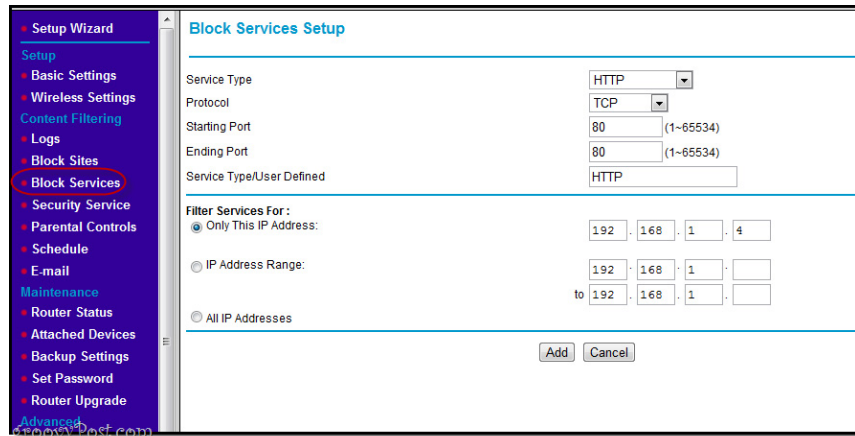


At the bottom of the admin page, the user can assign a **Trusted IP Address** parameter - 'trusted' IP addresses, in which case we do not want to block ourselves from those websites, but more simply. just the children in the family. Remember that our IP address here is **192.168.1.6**, so you can assign full access right here. However, you need to be careful when applying this method, because others can change the rules completely if they know how to do it basically. To check it again, let's try to access a website that is on the block list, and see what happens:

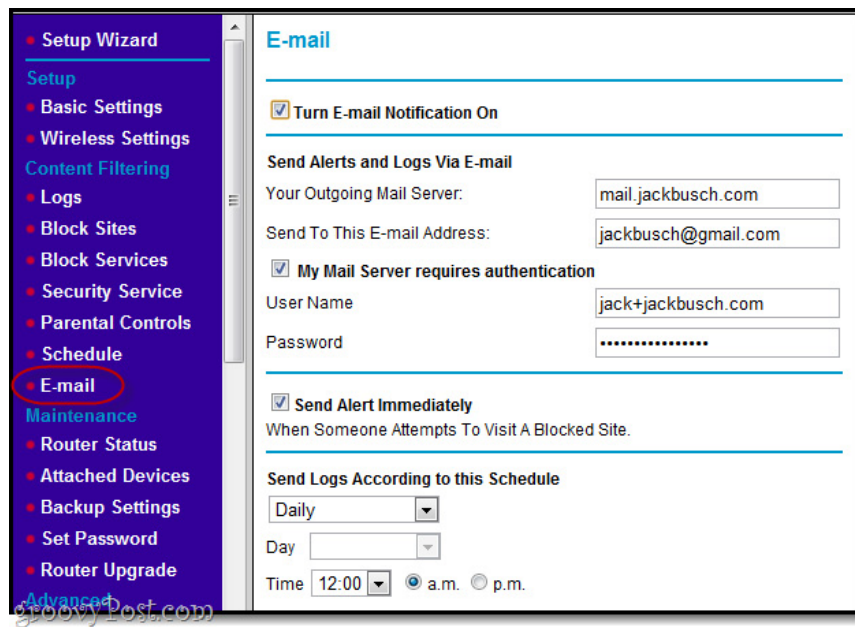


However, you also have to take into account the case where users do not access by normal address, but through IP address (for example, to access **Facebook** , just type **69.63.189.11** instead of **facebook.com** as usual). rate). To prevent this process, please add the corresponding IP address to the **Block** list.

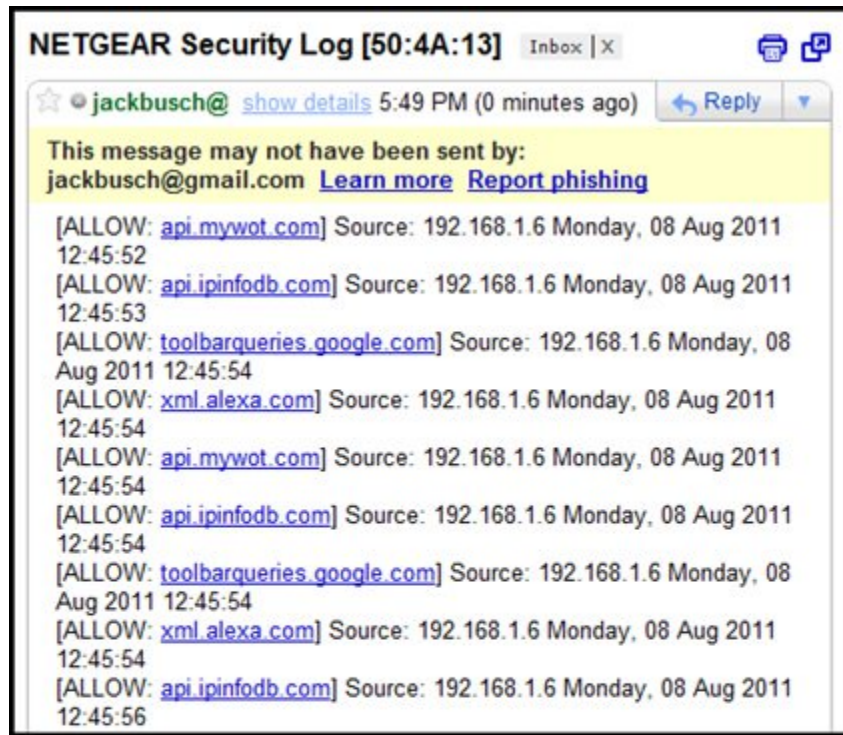
Tip: if you want to block all Internet access, for example after 9pm, then on the **Block Services** tab, select HTTP from the dropdown list, and make sure the IP address is determined with the same device. application:



When using the E-mail function, you can set the router to automatically email users of log files by hour, day, week or every time someone tries to access blocked websites. Or send the log file manually from the Logs page:



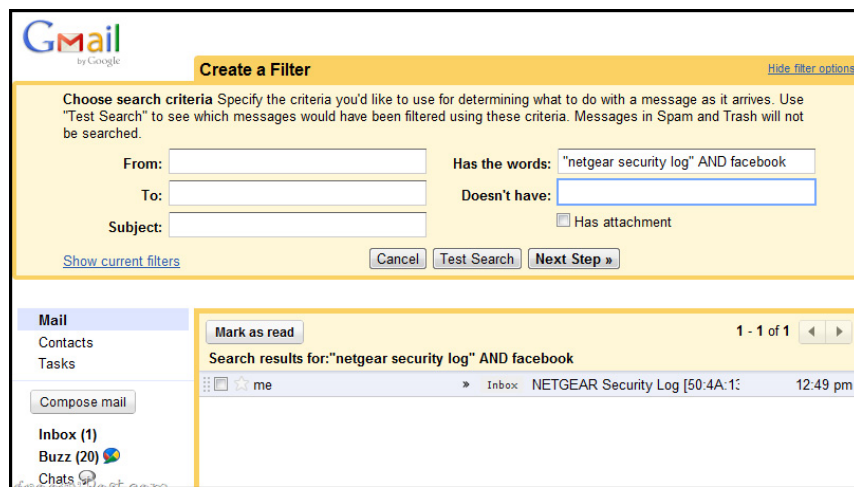
However, these emails often fall into **Spam** or **Junk** in the mailbox, so check carefully or set up the filter - **Filter** at this step:



These look phishy to Gmail, so be sure to mark it as "NOT SPAM."

groovyPost.com

What we are doing here, besides blocking websites, is the process of setting up the **Gmail Filter by itself** to check log files based on certain keywords and rank through the Star function:



With these filtering systems, users can receive full reports sent by day based on activities and information collected from family members when using the computer.

The use of security functions on NETGEAR's routers, as well as others, allows users to manage and monitor the entire amount of traffic data in the network after it is set up. The advantage of this approach is that there is no need to install any supporting software, however, the limitation of this method is that we cannot monitor any action on a smartphone or tablet device over the network. Mobile data (3G and 4G standards).

Good luck!

You finished reading the article "**Monitor your child's activity through the Wireless Router**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.