Internet connection management

There are many ways to manage Internet connection, depending on network size, importance of data and user level. From the simple security settings available in web browsers to solutions 'big hammer', look at

There are many ways to manage Internet connection, depending on network size, importance of data and user level. From simple security settings available in web browsers to solutions that are "big", we can generally solve this problem with software, hardware or use in combination. both.

There are a lot of network monitoring software on the market today, but to be most effective you need to equip more machines, technical staff to manage and even quite large copyright costs. You can also use a hardware solution such as a dedicated firewall (firewall) device or a router with a firewall. In addition to the ability to manage connections, some routers also have utilities to increase the security of network systems such as preventing denial attacks, locking data sharing services over the network, filtering website content . Good prizes. "all in one" solution not only saves you costs but also saves work space. This solution is suitable for small businesses and home users.

For convenience, we use a firewall that integrates DrayTek's Vigor 2800VG router. You can find more information about this router in the article "ADSL 2/2 + Multipurpose Router" (ID: A0612_90). In addition to the firewall utility, this product also integrates policies to prevent Denial of Service Denial of Service (DoS / DDoS) attacks, block sharing services, chat services, websites listed as "unnecessary" With filter mode in the form of Call filter and Data filter, or with SurfControl (30-day trial) users can filter website content by pre-classified topics .

Notes :

- Not all routers have the utilities and features we mentioned in the article.

- To ensure the security of the network, we should set up a mechanism to prevent denial of service attacks for the router and assign fixed IP to computers with Internet connection.

- Readers can refer to knowledge of IP address, TCP / IP protocol in Cisco CCNA syllabus or at http://www.vovisoft.com/mcse/rks/tnt/TCPIP.htm

Anti-DoS / DDoS attack

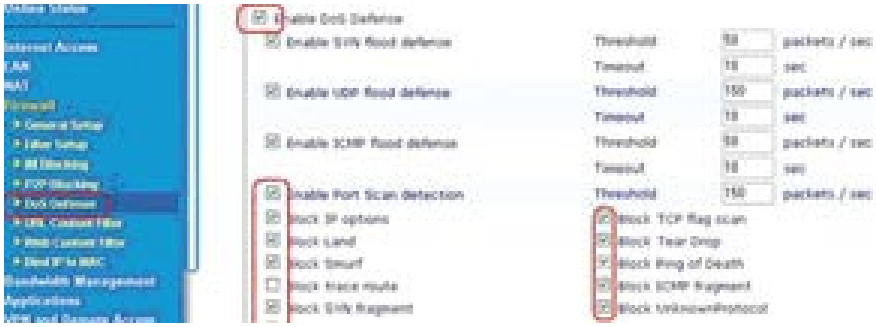

Figure 1 .Establish attack prevention mechanism

Denial of Service (DoS) attacks and distributed denial of service (DDoS) attacks are a problem for network administrators because they do not have absolute protection. However, you can enable this feature in the router to limit any harm when attacked. Set up as follows:

- In Internet Explorer, enter the address 192.168.1.1 (the default address with Vigor 2800VG router) and press Enter. Enter the administrator account name and password to enter the router's management interface (refer to the router's documentation).

- In the Firewall.DoS Defense section, check the Enable DoS Defense check box to activate (Figure 1).

Assign fixed IP to the computer

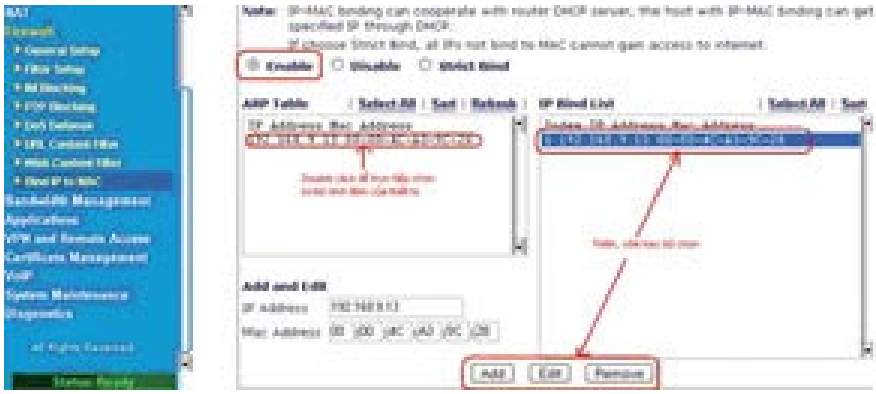

Figure 2 .Assign a fixed IP address

Routers typically have dynamic IP address allocation (DHCP Server), but for ease of control as well as to avoid confusion when blocking, we should assign a fixed IP address to computers that need to be managed.

First, we will check the IP address we are using through the computer name (each machine usually has a unique name set by the administrator). Once you have identified the IP and hostname, in the router's management interface, the Bind IP to MAC section, select Enable and select the corresponding IP address before clicking Add (Figure 2).

Prevent online games

Perform blocking by prohibiting connection to the IP address of the game server (game server). Depending on your ability, knowledge and experience, you will know the IP address of the game server.

Use NAT Session Table in the Diagnostic section to view the current Internet connection of computers on the network. For example, the computer has the IP address 192.168.9.13 accessing IP address 222.255.12.223 and 222.255.12.245. After checking the information, you know that this is the address of the servers in the SWTB game. A game will have multiple servers and IP addresses often change in the 4th cluster (223, 245 .). To quickly select, we will block words in the range 1 to 254 but if conditions permit, please monitor each game server specifically to prevent more accurately.

Set filter rules

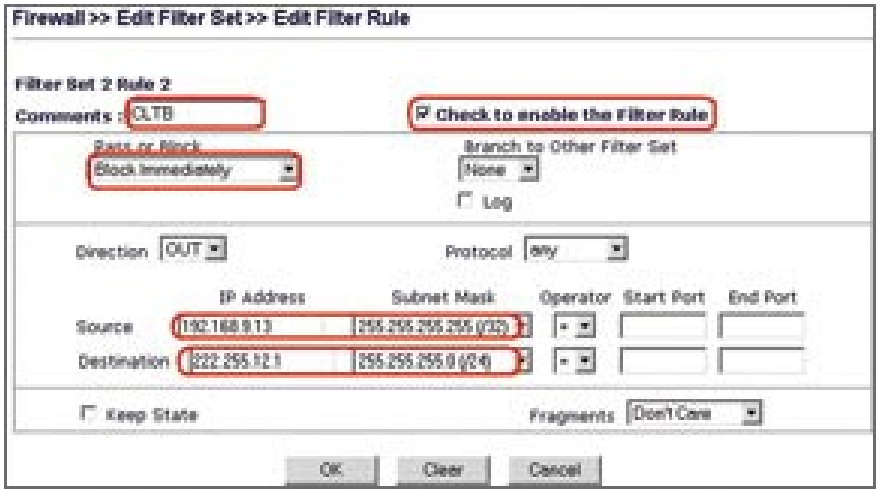

Figure 3 : Setting filter rules

In the management interface, select the Filter Setup item in the Firewall. You can select any Set in this section. Here we will select Set 2 (default data filter) and Fiter Rule 2 (because Filter Rule 1 is set by default). In the Comment box, you can make notes to make it easy to distinguish, for example, "cam game truc tuyen". With CLTB game, we will do the following:

• *Comment* : CLTB

• *Pass or Lock* : Block Immediately

• *Source* : IP of the computer that has assigned the MAC address. For example, 192.168.9.13, since only one IP address is banned, select Subnet Mask 255.255.255.0 (/ 32).

• *Destination* : type the address of the game server, because it is banned from 1 to 254, you will type 222.255.12.1, select Subnet Mask 255.255.255.0 (/ 24). Click OK to finish the setup (Figure 3).

To enable blocking, in Firewall.General Setup, check the checkbox Enable DataFilter, Start Filter Set: Set # 2. After setting up, the computer will not be able to connect to the CLTB game server. To remove, you only need to return the default settings of that set.

Filter by internal IP address

Figure 4: Filtering services by internal IP address

Similar to blocking online games, you can manage connections based on IP addresses of computers on the local network. A highly customizable filter allows network administrators to apply a customized policy simply and efficiently. For example, the accounting department's machines are not allowed to connect to the Internet. The IP address of the accounting room computer is 192.168.9.34 and 192.168.9.35. We will set up in the Data Filter, the Filter Setup section (Figure 4). In addition, we can prevent access based on connection ports (ports).

Chat service lock

Figure 5 : Prevent chat services

Chat (IM) is one of the most effective ways to exchange information. It's faster and more convenient than email and phone. However, chat abuse is a waste of time and reduces productivity. Therefore, you can block this service if necessary. To block chat, in Firewall select IM Blocking. Check Enable IM Blocking and set the allowable or blocking schedule in the Time Schedule section (Figure 5).

Peer sharing lock

Figure 6 : Preventing peer-to-peer network sharing

Sharing data in peer-to-peer (peer-to-peer or P2P) takes up quite a bit of bandwidth, which can even block the entire system. Moreover, when sharing peer to peer, the risk of network attacks is very high.

In Firewall, select P2P Blocking. Check the option Enable P2P Blocking and select the types of sharing to lock (Figure 6).

Filter web pages with keywords

Figure 7 .Filter the service with the URL

First, select the URL Content Filter item to enable this feature. Enter a representative keyword and all sites with related terms from the representative will be filtered. For example, if you enter the word "nhac", all pages such as *www.nhacso.net* , *www.nghenhac.info* , *tapchiamnhac.net* . will be banned from access (Figure 7). In addition, you can lock automatically run files like ActiveX .

Filter Web by topic classified by SurfControl

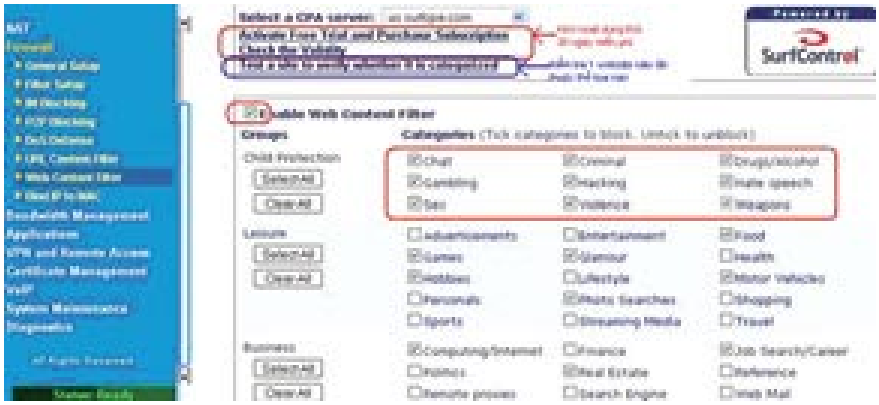

Figure 8 .Filter services with SurfControl

You can perform thematic site filtering already categorized by SurfControl - one of the world's leading website analytics and classification providers. For example, you can only allow access to websites to study, watch movies, or just allow access to news, news . but not access pages related to politics . all Both can be done easily with a few clicks (Figure 8).

Minh Quan

You finished reading the article "**Internet connection management**" 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.