Anti-DDoS Firewall

User's Manual

How to configure and use FortGuard Professional Anti-DDoS Firewall

http://www.fortguard.com

Regarding Installation

Installation notes:

FortGuard firewall can run stably on Windows 2000 Server and Windows 2003 Server systems. To avoid conflict, please ensure that neither other firewall software nor hook anti-virus software is installed. In fact, other types of packet filtering firewall can not contribute to anti-DDoS. Some can even put heavy burden to the system. For the same reason, hook antivirus software will degrade system performance severely and affect system stability negatively.

In another word, do not install on the server with security software only suitable for individual PCs. If you are lack of confidence in the security of your servers, feel free to contact us for help. Our security engineers will provide you with free advice.

Regarding Installation(2)

Failure in installation:

It is most likely caused by the conflict between FortGuard and other security software. If unloading other security software can not help to start FortGuard DDoS Firewall successfully, there would be some other factors.

Please feel free to contact our technical support engineers to solve the problem.

Regarding Installation(3)

Upgrade installation:

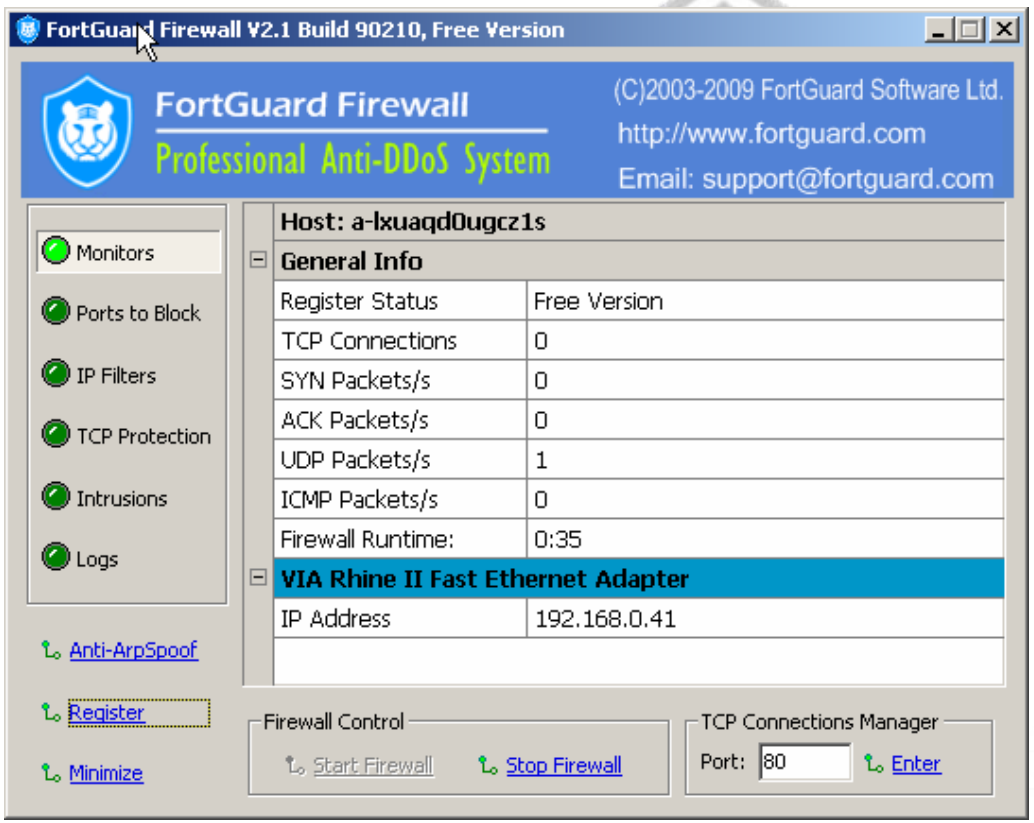
Uninstall the old version of FortGuard Anti-DDoS firewall first, and restart you system.

Install the new version, and restart the system to use the updated firewall for Windows 2000 Server system.

For the Windows 2003 Server system, no need to restart the system to start FortGuard Anti-DDoS firewall.

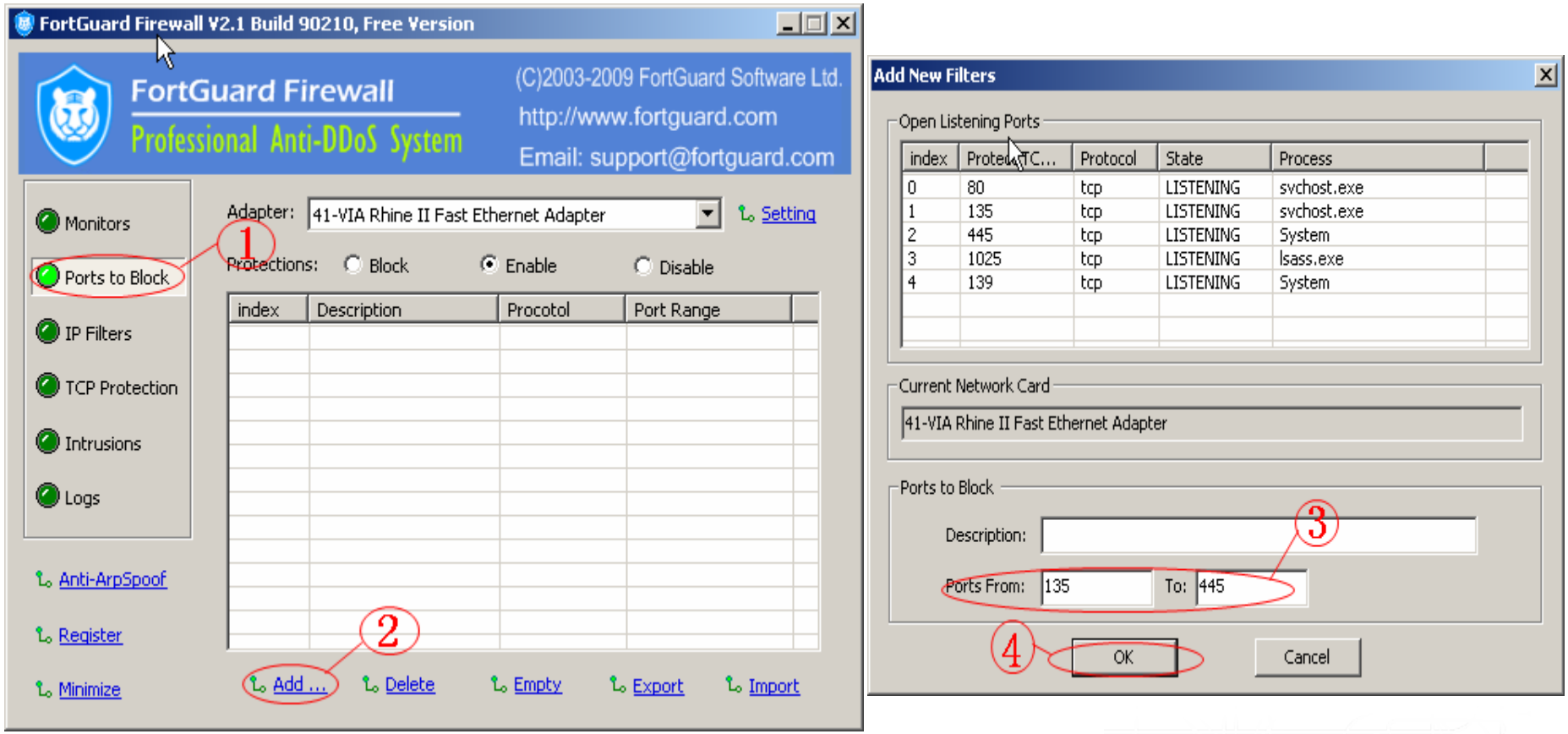
Status monitors

Here you can see the registration status, TCP connections, SYN packets/s, ACK packets/s , UDP packets/s, ICMP packets/s, Firewall runtime, IP address etc.. When suffering evil TCP connection flooding or evil http request flooding attacks, TCP connections number will reach to a very high volume, several thousands or even more; when suffering SYN UDPFLOOD attacks, the volume of the UDP and SYN attacks will rise constantly.



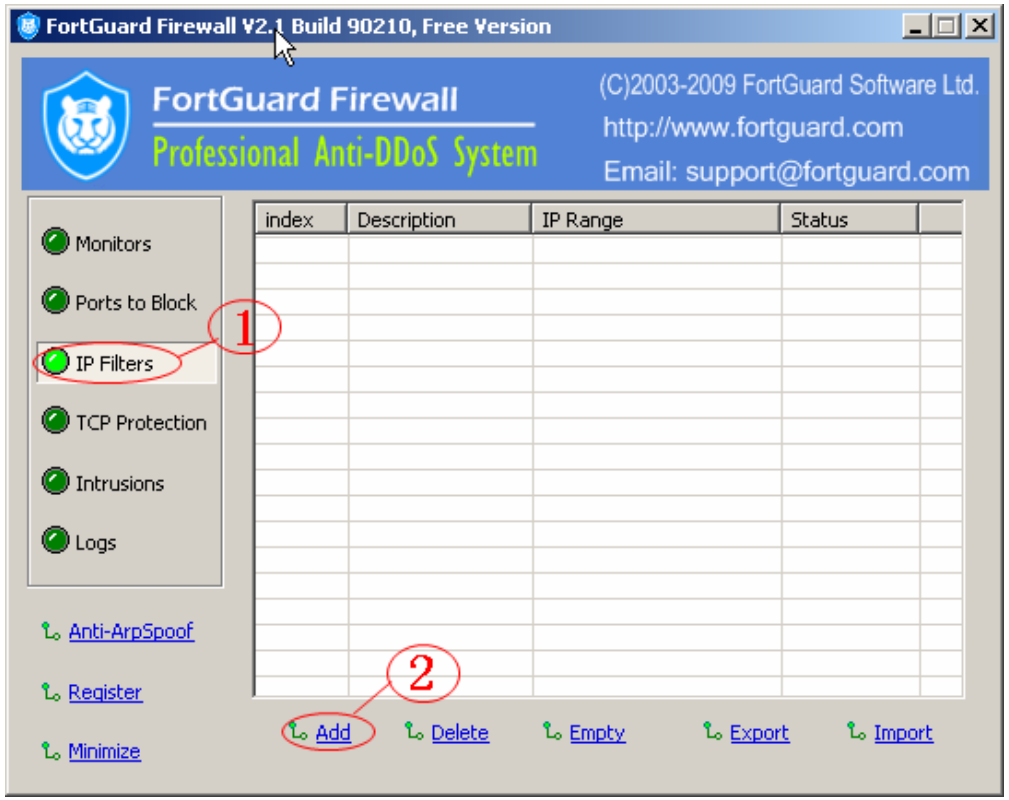
Ports to Block

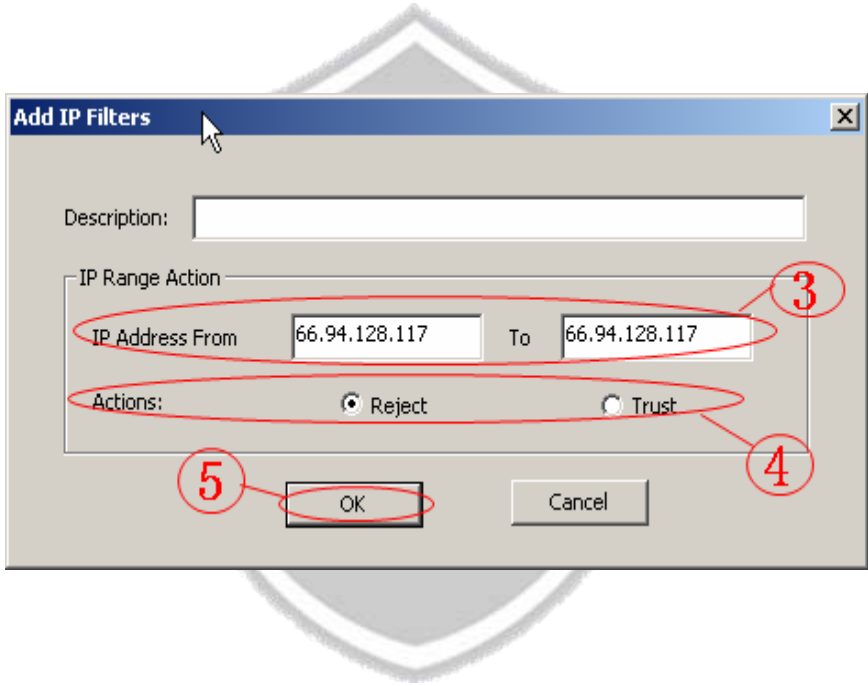
Here displays the protection status of the current internet adaptor. Here you can block a certain port or a port range.



IP Filters

IP Black list / White list. Reject an IP or an IP range; trust an IP or an IP range.

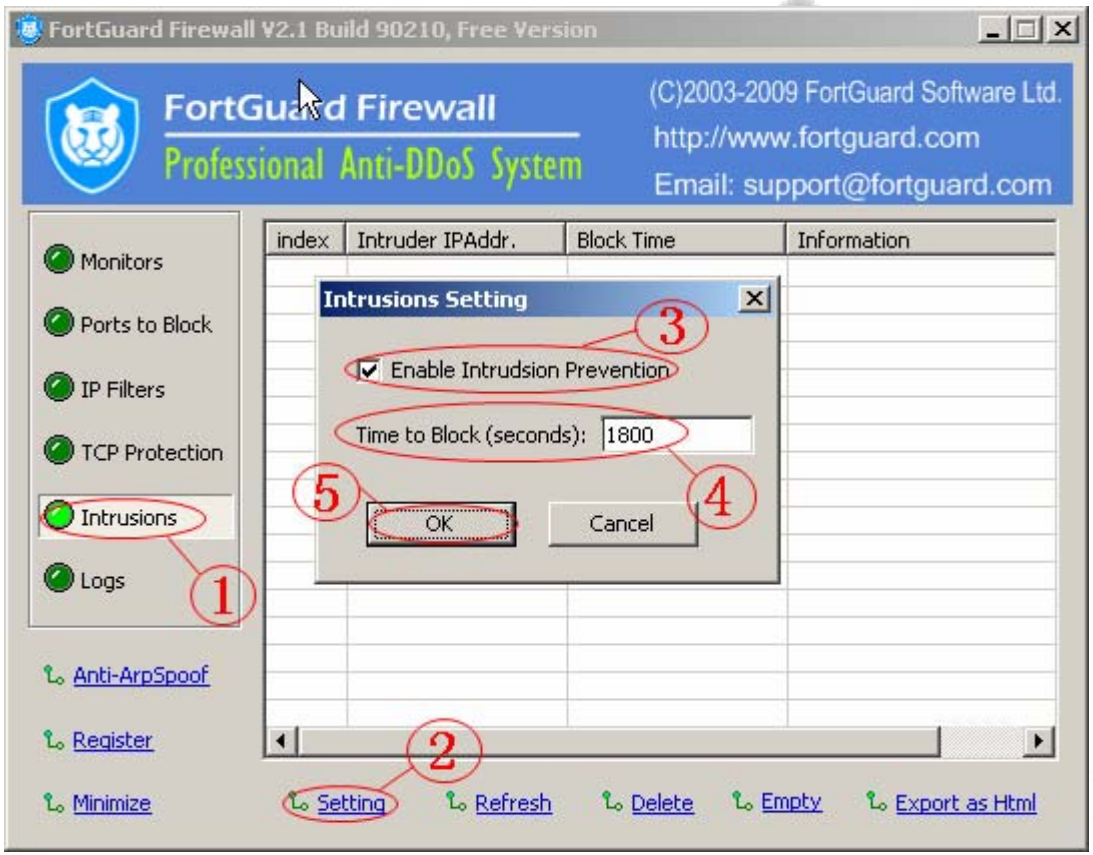




Intrusion Prevention

Proactively block Network worms, spyware, overflow attacks, database attacks, network equipment attacks and other attacks and make up for the effectiveness in deep defense from other security products.

(1) Click “ Intrusions ”, (2) Click “Setting”, (3) Select “Enable Intrusion Prevention”, (4) set “Time To Block (seconds)” to “1800” , (5) Click “ OK”.

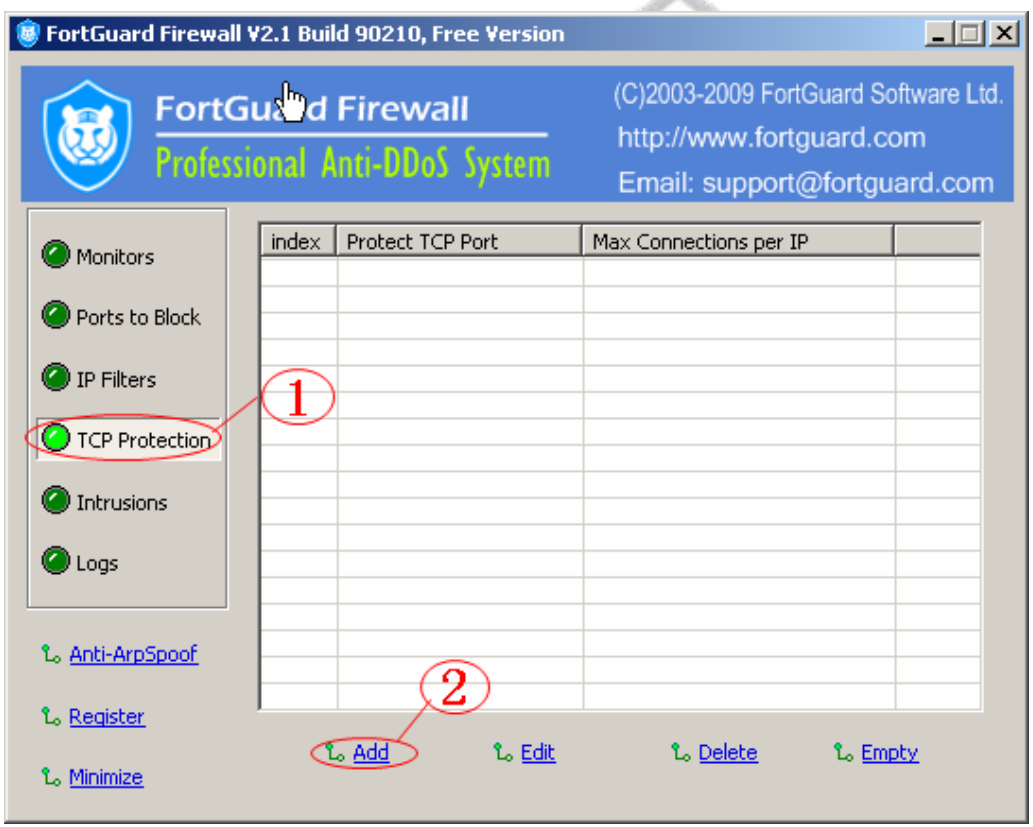


TCP Flow Control

TCP protection set up manually: If you are suffered with evil TCP connection flooding and evil http request flooding attacks:

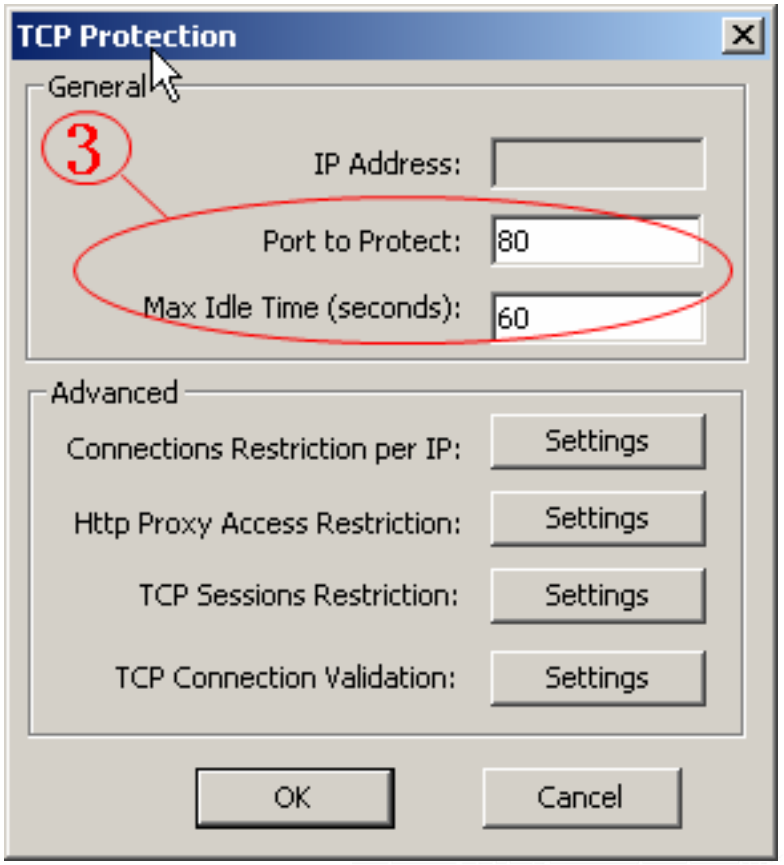
The following example illustrates TCP settings when port 80 suffers general TCP flood attacks:

(1) Click "TCP protection", (2) and then click "Add".



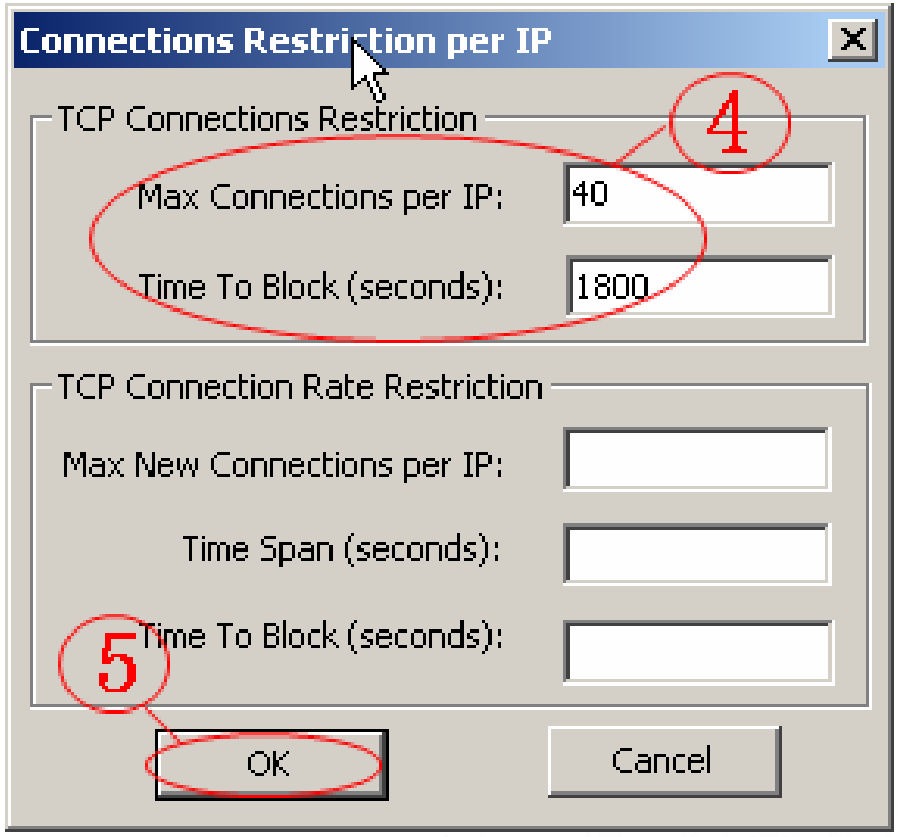
TCP Flow Control (2)

（3）Input “80” at “Port to Protect ”; Generally input “60” at “Max Idle Time (seconds)”.



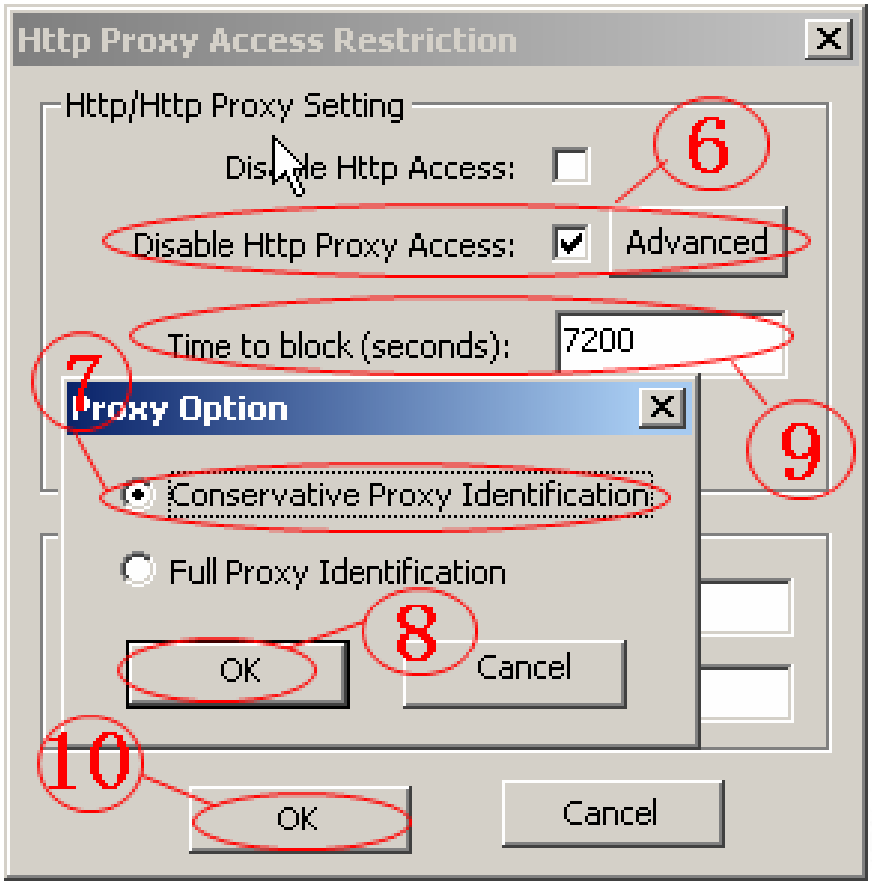
TCP Flow Control (3)

(4) click “settings” button after “Connections Restriction per IP”; set “Max Connections per IP” to “40”; set “Time To Block (Seconds)” to “1800” in the pop-up dialog box; (5)click “ OK ”.



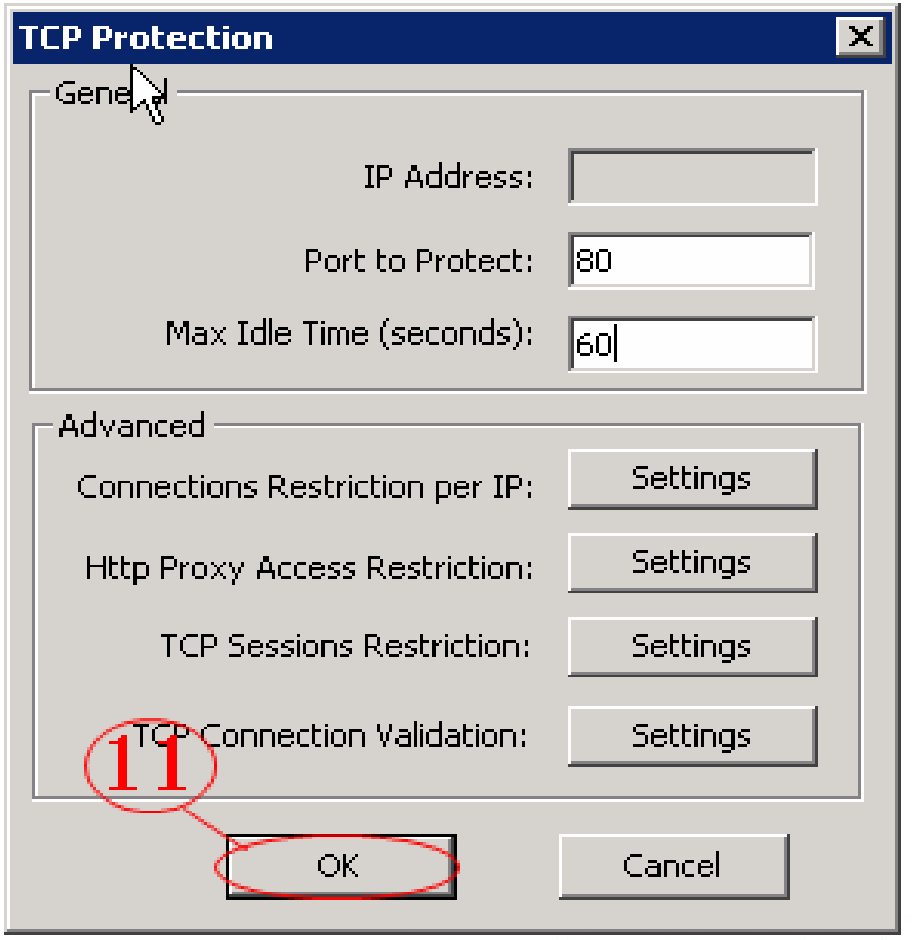
TCP Flow Control (4)

(6)Click “setup” button after “HTTP Proxy Access Restriction”, select “Disable Http Proxy Access”; click “Advanced” button; (7)select “Conservative Proxy Identification” in the pop-up dialog box “Proxy Option”; (8)click “OK” button; (9)set “Time to block (seconds)”as“7200”; (10)click “OK” button.



TCP Flow Control (5)

(11) click “OK” button.



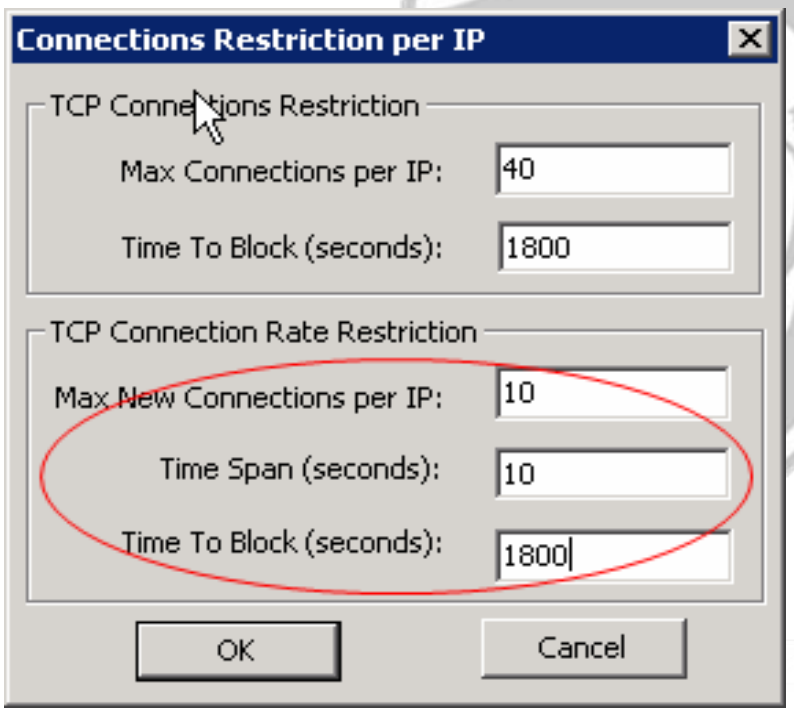
TCP Flow Control (6)

If you are suffered with severe evil TCP connection flooding and evil http request flooding attacks:

(1) First，finish the settings of TCP Control (1), (2), (3), (4), (5)

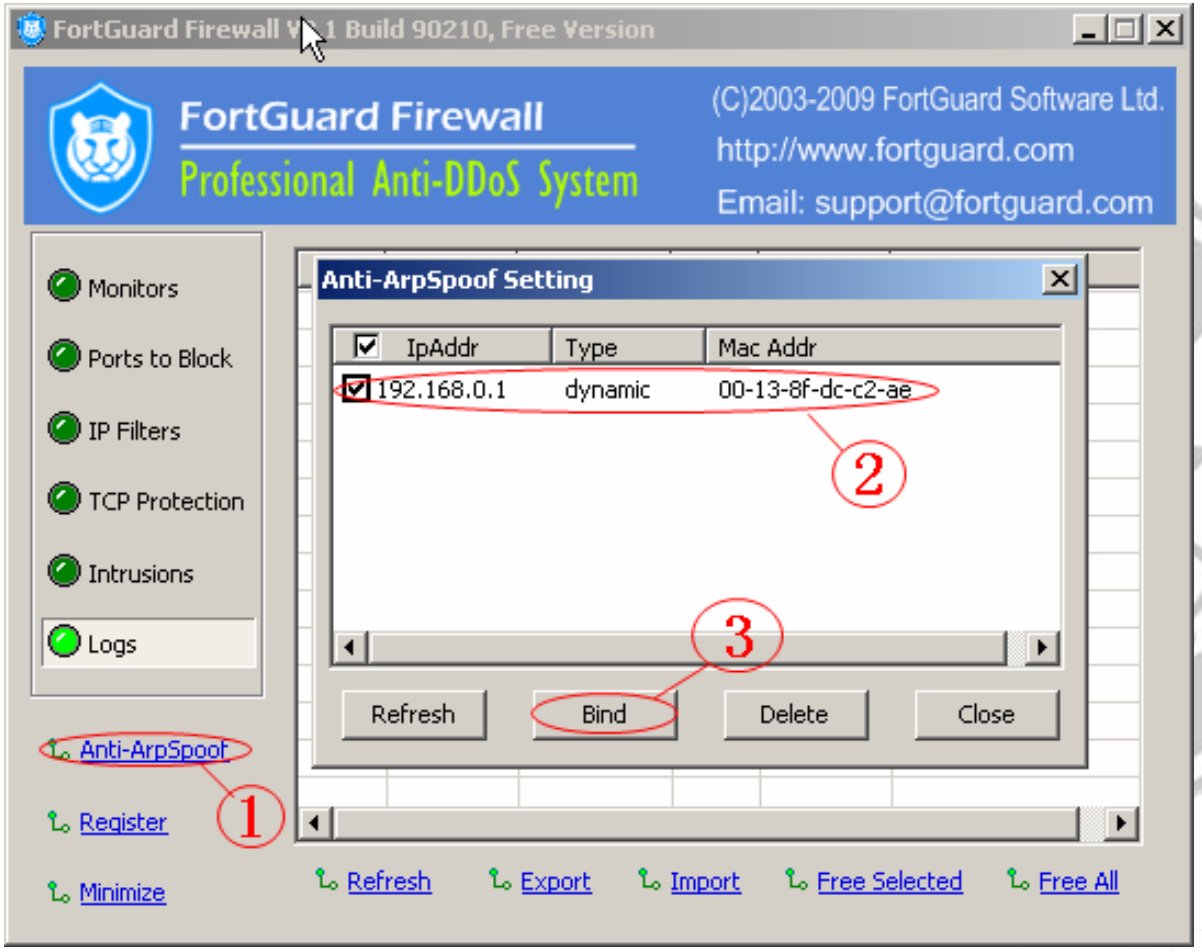
(2) Second, according to the attack condition, set “Tcp Connection Rate Restriction” to satisfy the protection requirements.

For example, set “Max New Connections per IP” to “10”; set “Time Span (seconds)” to “10”; set “Time To Block (Seconds)” to “1800”; click “OK” button.



Anti-Arpspoof

If you are facing ARP spoofing attacks, click Anti-Arpspoof, select your internet adaptor, and then click Bind.



END

Thank you!

FortGuard SoftwareTechnology Co., Ltd.
http://www.fortguard.com
Sales: win@fortguard.com
Support: support@fortguard.com