



**FORTGuard** Anti-DDoS Firewall

# User's Manual

How to configure and use FortGuard Professional Anti-DDoS Firewall

Copyright © 2003-2009 FortGuard Software Technology Co., Ltd.

<http://www.fortguard.com>

## Installation notes:

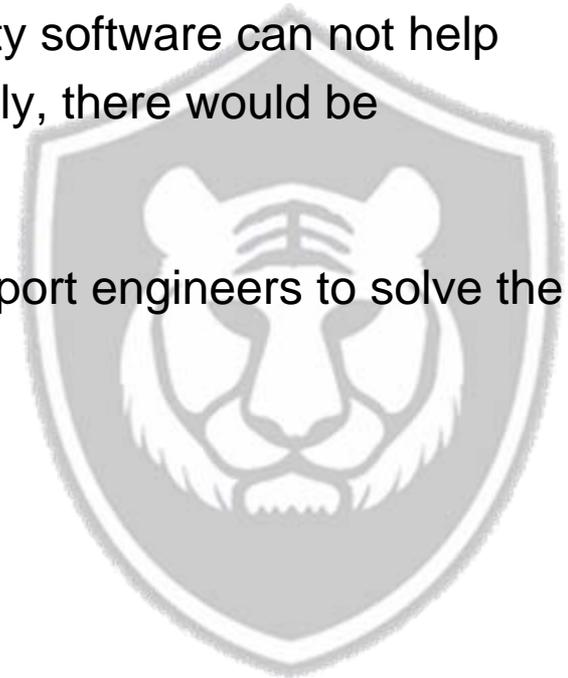
FortGuard firewall can run stably on Windows 2000 Server and Windows 2003 Server systems. To avoid conflict, please ensure that neither other firewall software nor hook anti-virus software is installed. In fact, other types of packet filtering firewall can not contribute to anti-DDoS. Some can even put 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.

## 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.

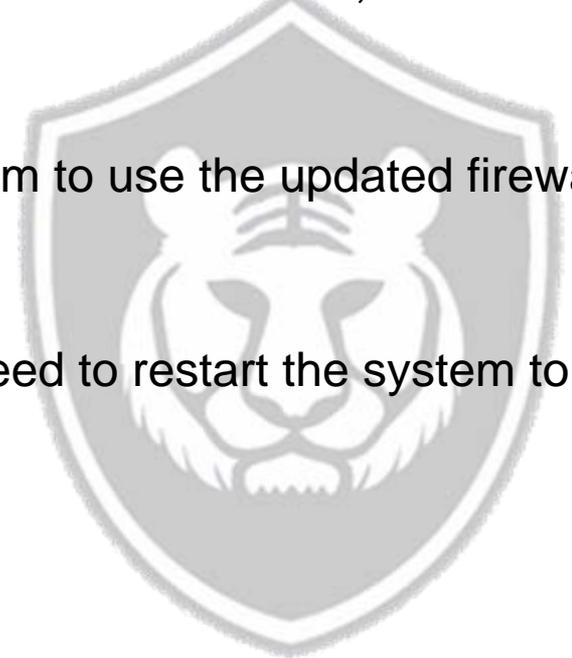


## Upgrade installation:

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.

The screenshot shows the FortGuard Firewall V2.1 interface. The title bar reads "FortGuard Firewall V2.1 Build 90210, Free Version". The main header includes the FortGuard logo, the text "FortGuard Firewall Professional Anti-DDoS System", and copyright information: "(C)2003-2009 FortGuard Software Ltd. http://www.fortguard.com Email: support@fortguard.com".

On the left, a sidebar contains several status monitors, each with a green indicator light:

- Monitors
- Ports to Block
- IP Filters
- TCP Protection
- Intrusions
- Logs

Below the sidebar are links for "Anti-ArpSpoof", "Register", and "Minimize".

The main content area displays "Host: a-lxuaqd0ugcz1s" and a "General Info" table:

Register Status	Free Version
TCP Connections	0
SYN Packets/s	0
ACK Packets/s	0
UDP Packets/s	1
ICMP Packets/s	0
Firewall Runtime:	0:35

Below the table, the interface shows "VIA Rhine II Fast Ethernet Adapter" with an IP Address of 192.168.0.41.

At the bottom, there are two control panels:

- Firewall Control:** Includes "Start Firewall" and "Stop Firewall" buttons.
- TCP Connections Manager:** Includes a "Port:" field with the value "80" and an "Enter" button.

# Ports to Block



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

FortGuard Firewall V2.1 Build 90210, Free Version

FortGuard Firewall  
Professional Anti-DDoS System

(C)2003-2009 FortGuard Software Ltd.  
http://www.fortguard.com  
Email: support@fortguard.com

Adapter: 41-VIA Rhine II Fast Ethernet Adapter [Setting](#)

Protections:  Block  Enable  Disable

index	Description	Protocol	Port Range

[Add ...](#) [Delete](#) [Empty](#) [Export](#) [Import](#)

Add New Filters

Open Listening Ports

index	Protocol	State	Process	
0	80	tcp	LISTENING	svchost.exe
1	135	tcp	LISTENING	svchost.exe
2	445	tcp	LISTENING	System
3	1025	tcp	LISTENING	lsass.exe
4	139	tcp	LISTENING	System

Current Network Card  
41-VIA Rhine II Fast Ethernet Adapter

Ports to Block

Description:

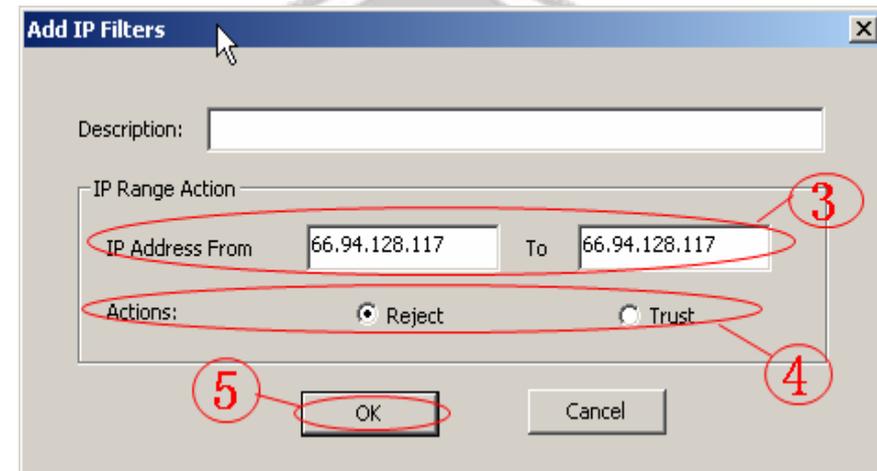
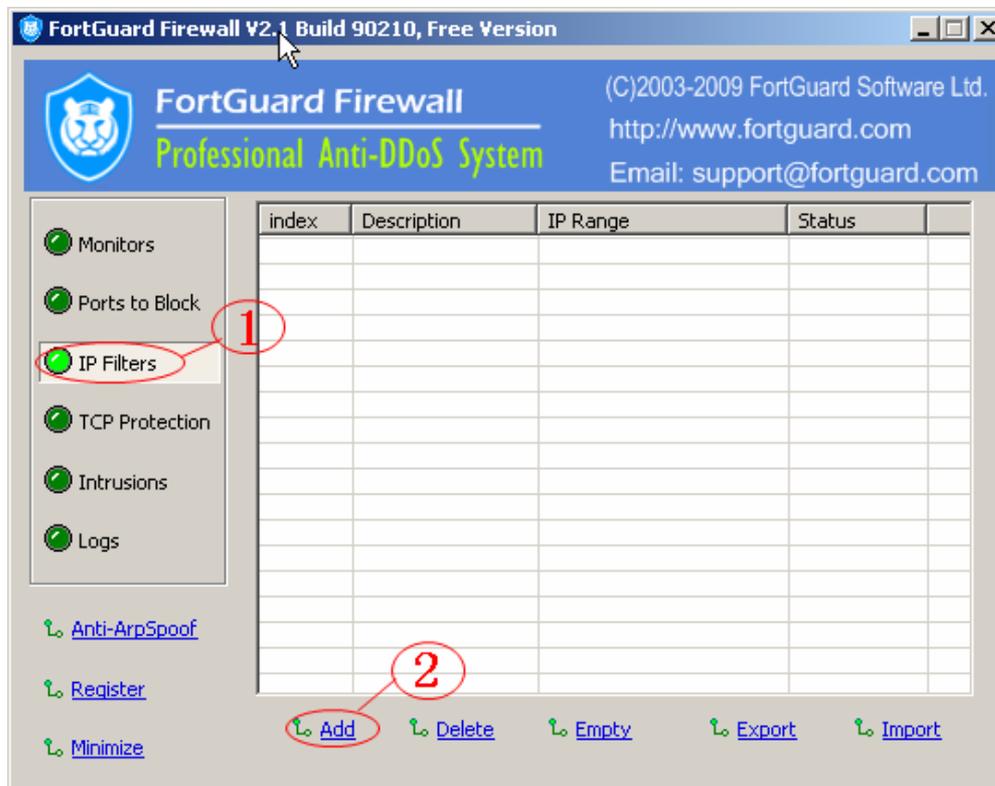
Ports From:  To:

OK  Cancel

# IP Filters



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







# TCP Flow Control (2)

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



**TCP Protection**

General

3

IP Address:

Port to Protect:

Max Idle Time (seconds):

Advanced

Connections Restriction per IP:

Http Proxy Access Restriction:

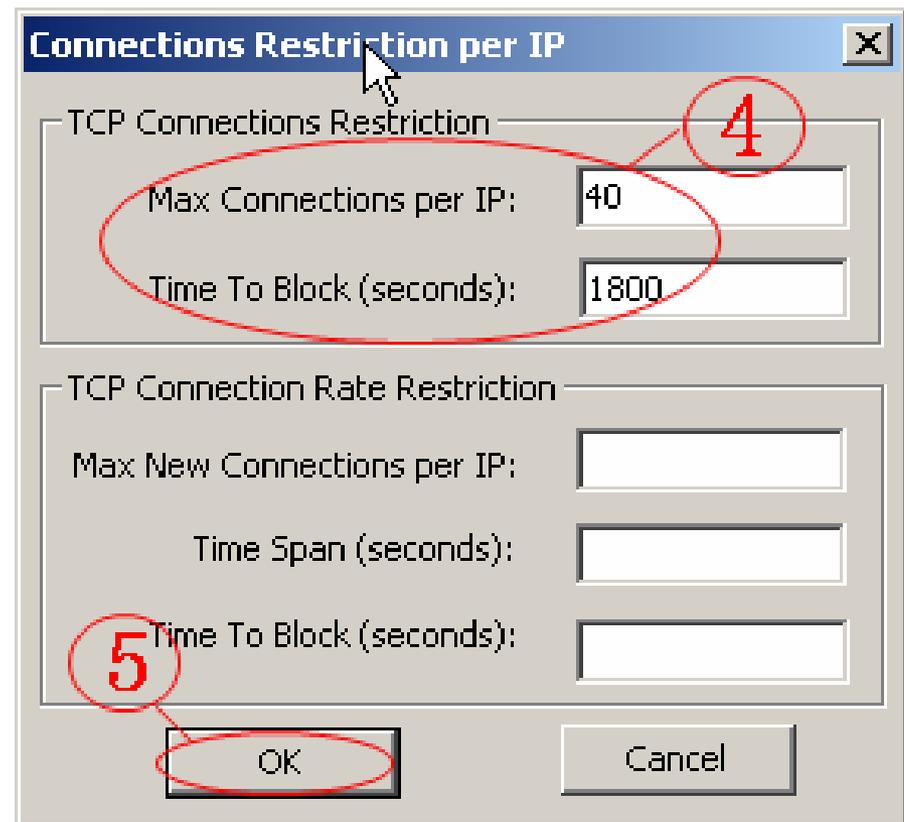
TCP Sessions Restriction:

TCP Connection Validation:

# TCP Flow Control (3)

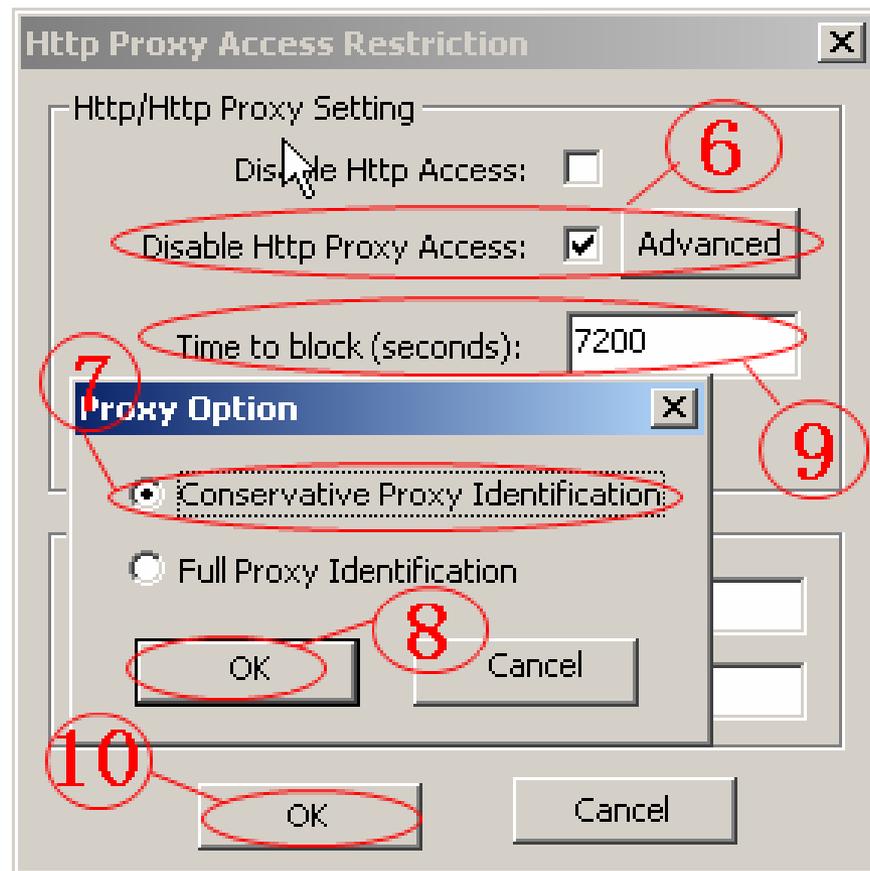


(4) click “settings” button after “Connections Restriction per IP”; set “Max Connections per IP” to “40”; set “Time To Block (Seconds)” to “1800” in the pop-up dialog box; (5)click “ OK ”.



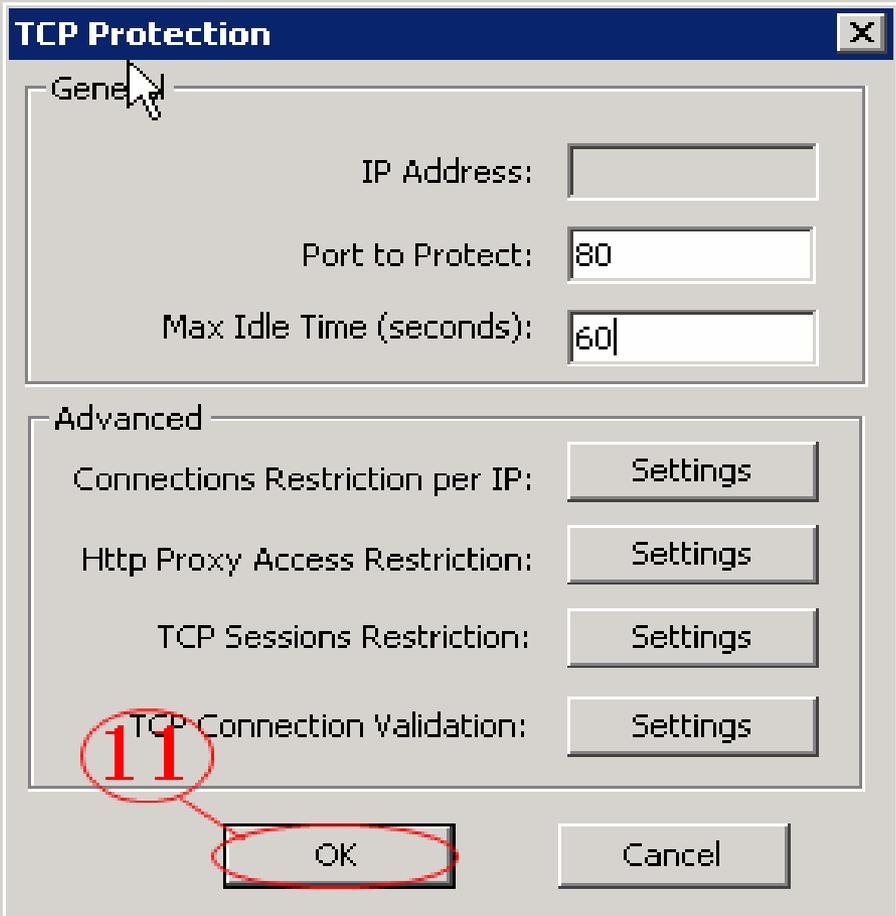
# TCP Flow Control (4)

(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 Protection**

General

IP Address:

Port to Protect:

Max Idle Time (seconds):

Advanced

Connections Restriction per IP:

Http Proxy Access Restriction:

TCP Sessions Restriction:

**11** TCP Connection Validation:

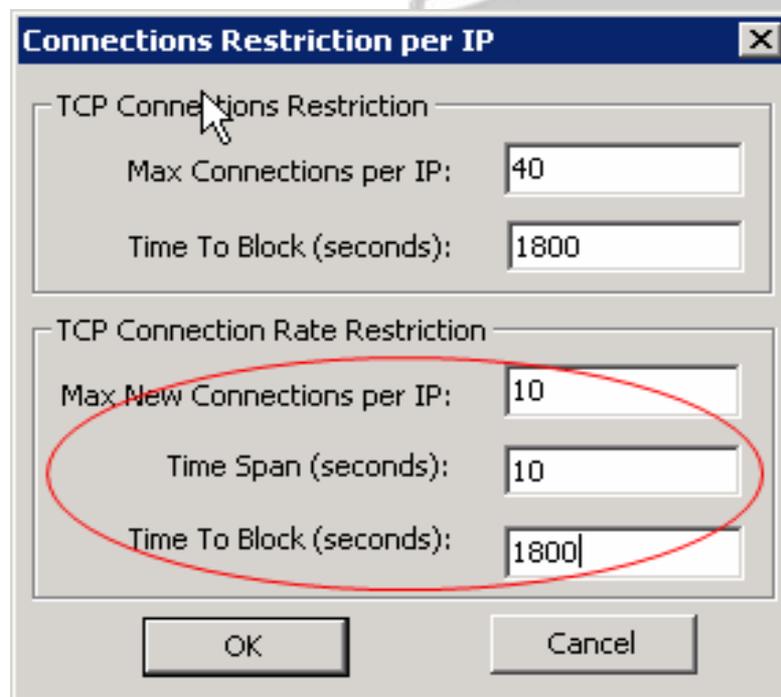
# TCP Flow Control (6)

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.



**Connections Restriction per IP**

TCP Connections Restriction

Max Connections per IP: 40

Time To Block (seconds): 1800

TCP Connection Rate Restriction

Max New Connections per IP: 10

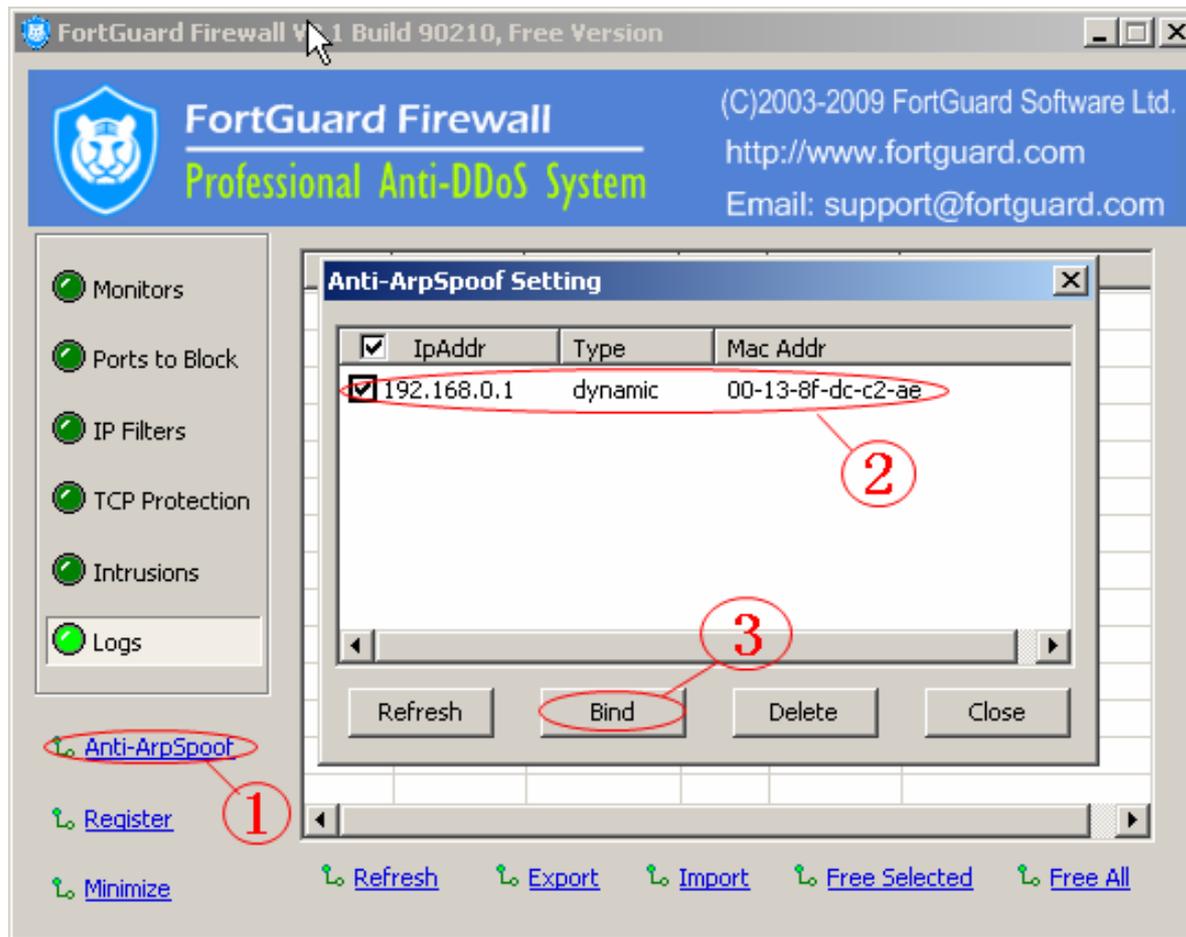
Time Span (seconds): 10

Time To Block (seconds): 1800

OK Cancel

# 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](mailto:win@fortguard.com)

Support: [support@fortguard.com](mailto:support@fortguard.com)

