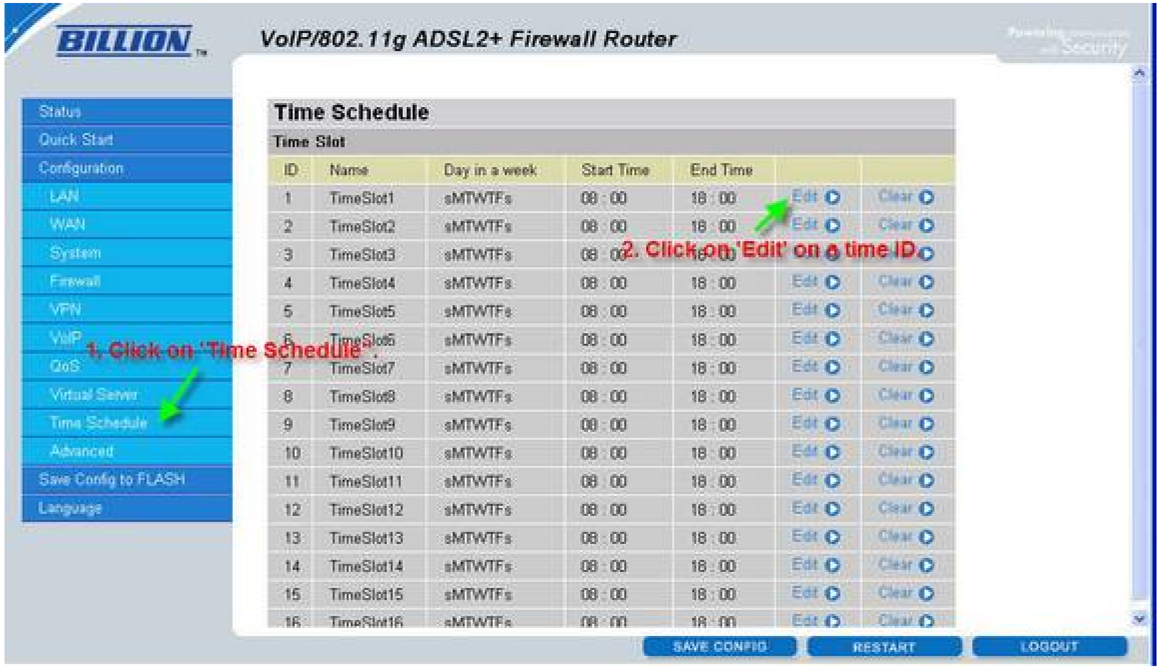
Time Restriction on IP address

To denial Internet access on a certain day and time on a specific IP address. The first thing to do is set the time schedule as follows:



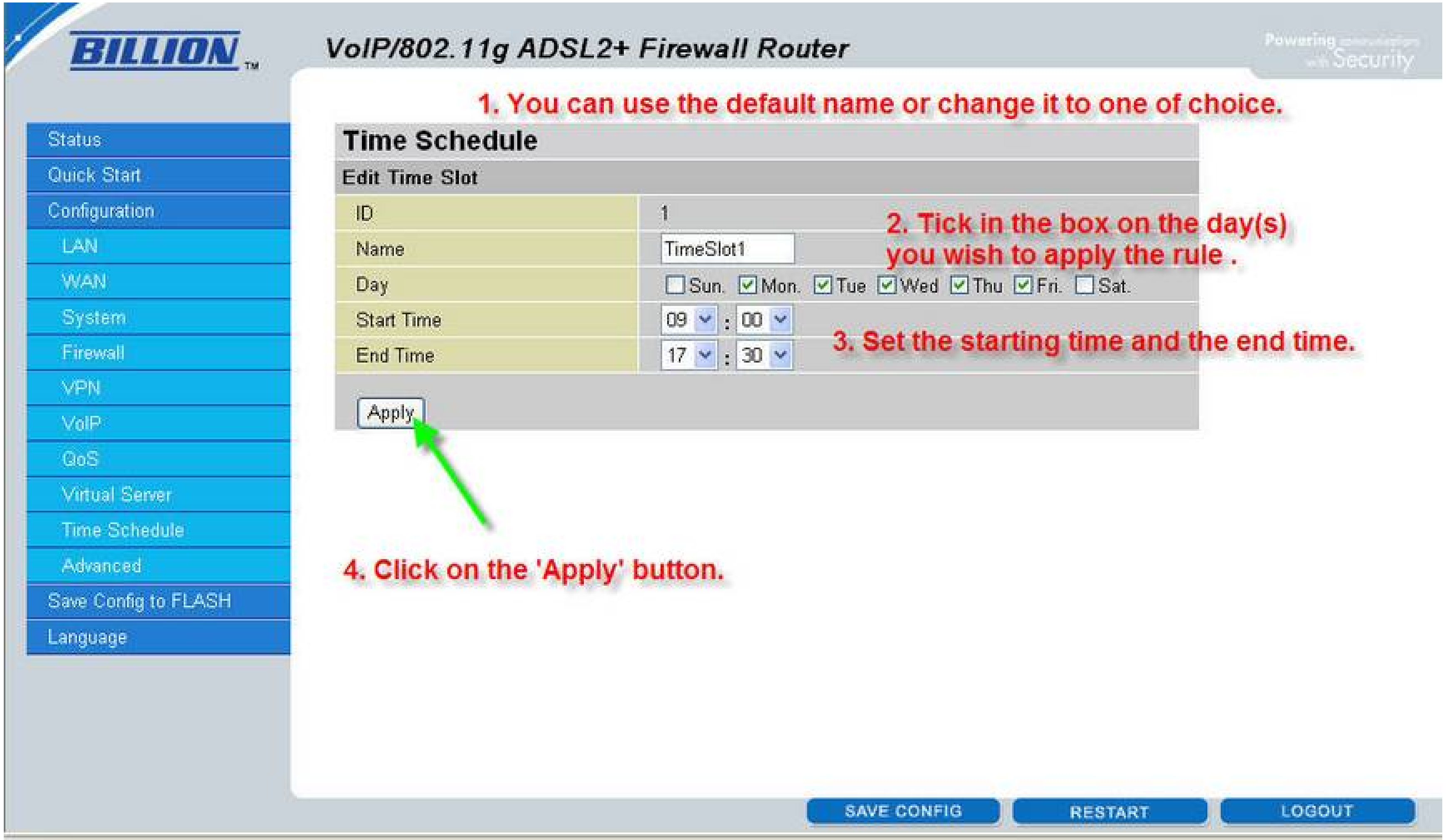
1. Click on 'Time Schedule'.

2. Click on 'Edit' on a time ID

Time Schedule

Time Slot

ID	Name	Day in a week	Start Time	End Time		
1	TimeSlot1	sMTWTFs	08 : 00	18 : 00	Edit	Clear
2	TimeSlot2	sMTWTFs	08 : 00	18 : 00	Edit	Clear
3	TimeSlot3	sMTWTFs	08 : 00	18 : 00	Edit	Clear
4	TimeSlot4	sMTWTFs	08 : 00	18 : 00	Edit	Clear
5	TimeSlot5	sMTWTFs	08 : 00	18 : 00	Edit	Clear
6	TimeSlot6	sMTWTFs	08 : 00	18 : 00	Edit	Clear
7	TimeSlot7	sMTWTFs	08 : 00	18 : 00	Edit	Clear
8	TimeSlot8	sMTWTFs	08 : 00	18 : 00	Edit	Clear
9	TimeSlot9	sMTWTFs	08 : 00	18 : 00	Edit	Clear
10	TimeSlot10	sMTWTFs	08 : 00	18 : 00	Edit	Clear
11	TimeSlot11	sMTWTFs	08 : 00	18 : 00	Edit	Clear
12	TimeSlot12	sMTWTFs	08 : 00	18 : 00	Edit	Clear
13	TimeSlot13	sMTWTFs	08 : 00	18 : 00	Edit	Clear
14	TimeSlot14	sMTWTFs	08 : 00	18 : 00	Edit	Clear
15	TimeSlot15	sMTWTFs	08 : 00	18 : 00	Edit	Clear
16	TimeSlot16	sMTWTFs	08 : 00	18 : 00	Edit	Clear



1. You can use the default name or change it to one of choice.

Time Schedule

Edit Time Slot

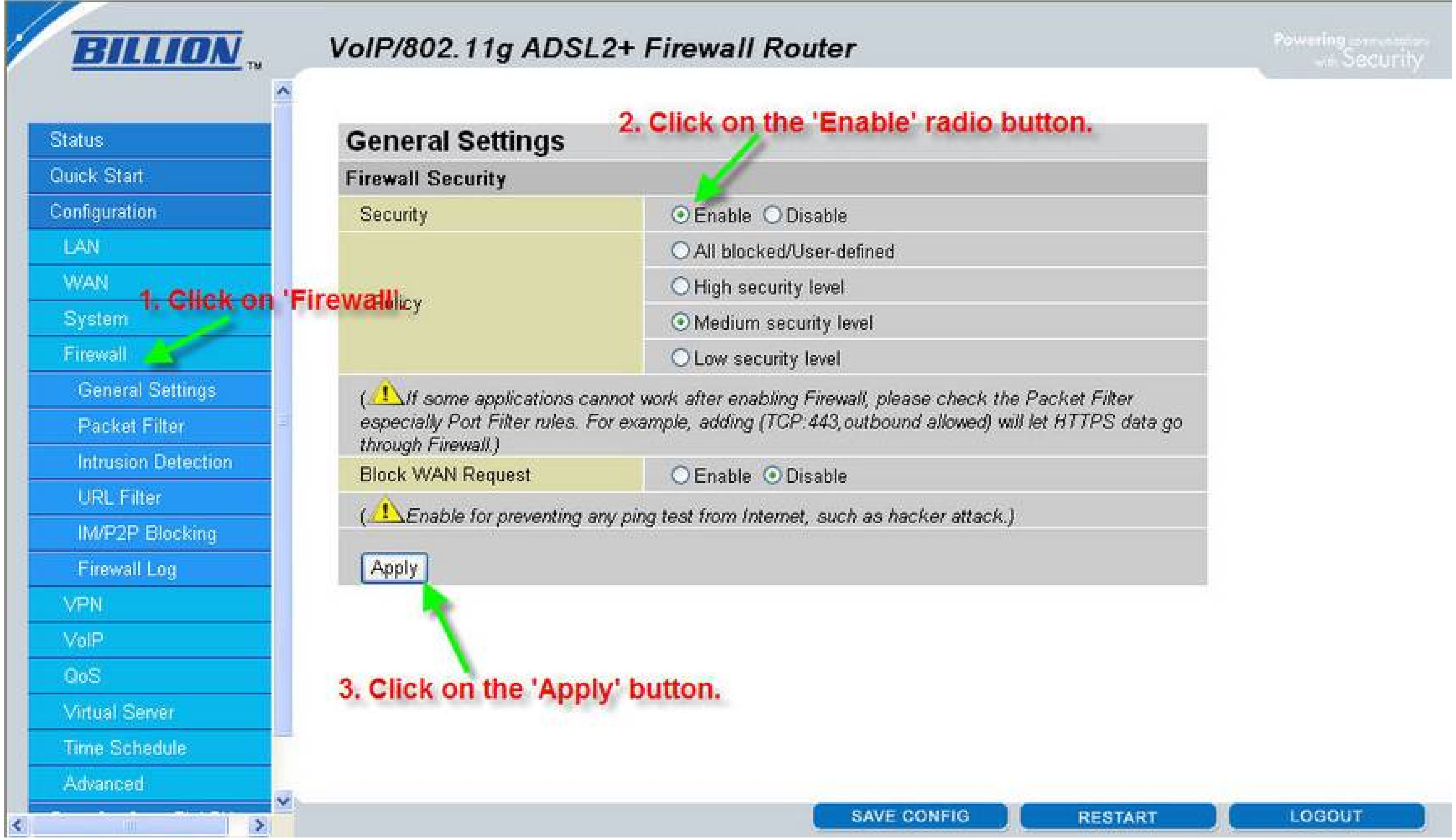
ID	1
Name	TimeSlot1
Day	☐ Sun. ☑ Mon. ☑ Tue ☑ Wed ☑ Thu ☑ Fri. ☐ Sat.
Start Time	09 : 00
End Time	17 : 30

2. Tick in the box on the day(s) you wish to apply the rule .

3. Set the starting time and the end time.

4. Click on the 'Apply' button.

Next you need to enable the firewall



1. Click on 'Firewall'.

2. Click on the 'Enable' radio button.

3. Click on the 'Apply' button.

General Settings

Firewall Security

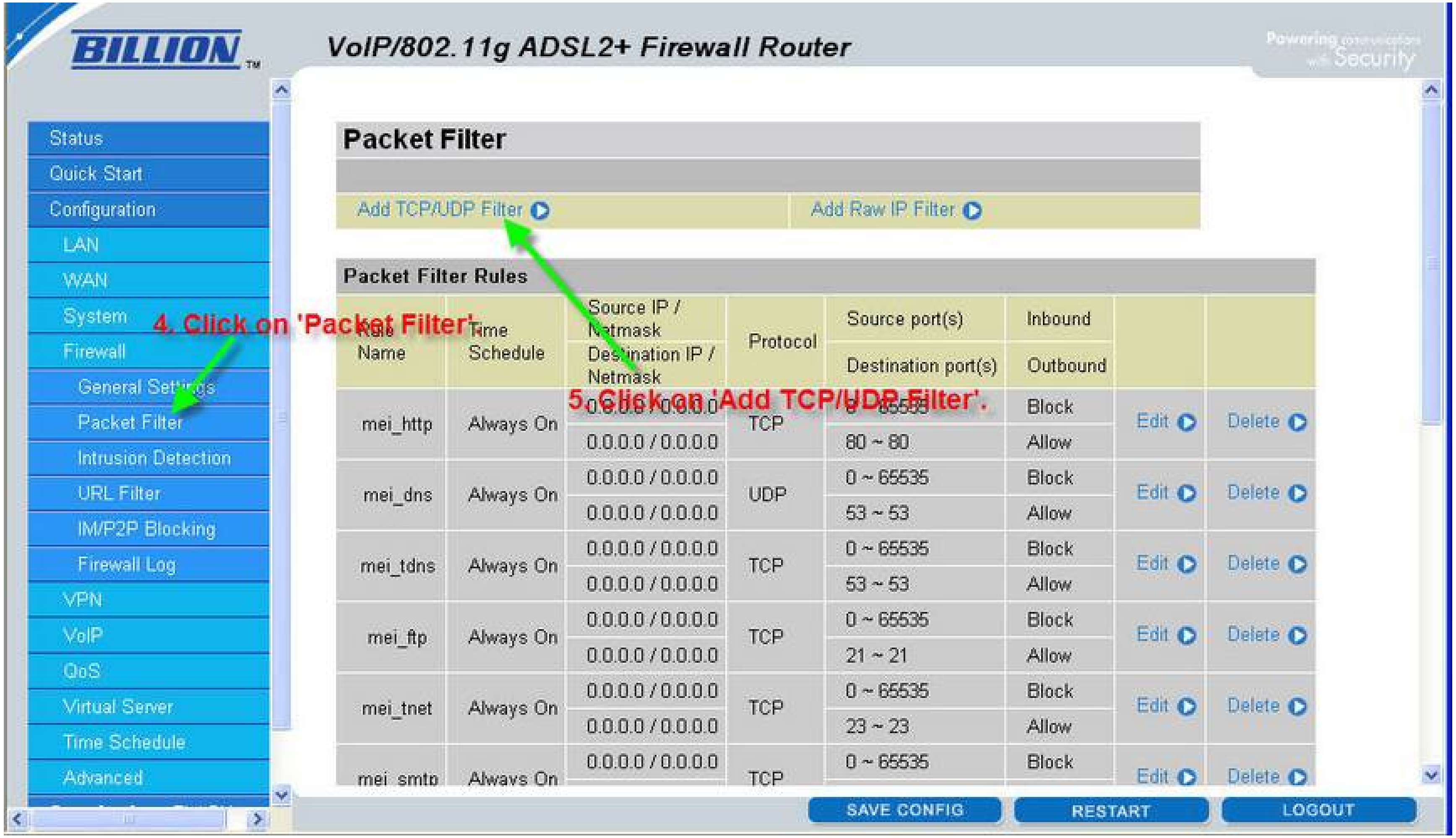
Security	● Enable ○ Disable
Policy	○ All blocked/User-defined ○ High security level ● Medium security level ○ Low security level

(⚠If some applications cannot work after enabling Firewall, please check the Packet Filter especially Port Filter rules. For example, adding (TCP:443,outbound allowed) will let HTTPS data go through Firewall.)

Block WAN Request	○ Enable ● Disable

(⚠Enable for preventing any ping test from Internet, such as hacker attack.)

Apply



4. Click on 'Packet Filter'.

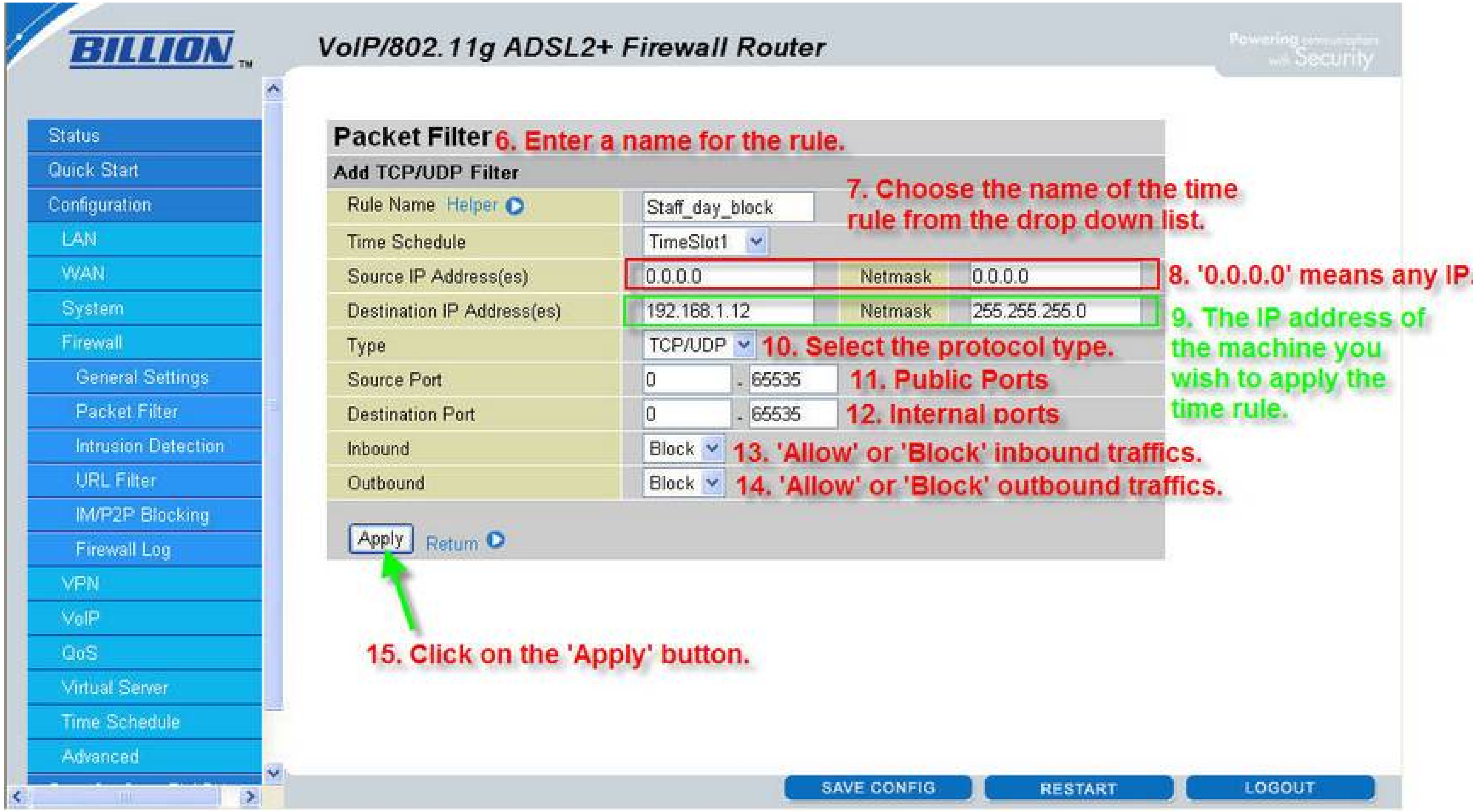
5. Click on 'Add TCP/UDP Filter'.

Packet Filter

Add TCP/UDP Filter ▶ Add Raw IP Filter ▶

Packet Filter Rules

Rule Name	Time Schedule	Source IP / Netmask Destination IP / Netmask	Protocol	Source port(s) Destination port(s)	Inbound Outbound		
mei_http	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		80 ~ 80	Allow		
mei_dns	Always On	0.0.0.0 / 0.0.0.0	UDP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		53 ~ 53	Allow		
mei_tdns	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		53 ~ 53	Allow		
mei_ftp	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		21 ~ 21	Allow		
mei_tnet	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶
		0.0.0.0 / 0.0.0.0		23 ~ 23	Allow		
mei_smtp	Always On	0.0.0.0 / 0.0.0.0	TCP	0 ~ 65535	Block	Edit ▶	Delete ▶



Packet Filter 6. Enter a name for the rule.

Add TCP/UDP Filter

Rule Name Helper	Staff_day_block		
Time Schedule	TimeSlot1		
Source IP Address(es)	0.0.0.0	Netmask	0.0.0.0
Destination IP Address(es)	192.168.1.12	Netmask	255.255.255.0
Type	TCP/UDP		
Source Port	0 - 65535		
Destination Port	0 - 65535		
Inbound	Block		
Outbound	Block		

Apply Return

7. Choose the name of the time rule from the drop down list.

8. '0.0.0.0' means any IP.

9. The IP address of the machine you wish to apply the time rule.

10. Select the protocol type.

11. Public Ports

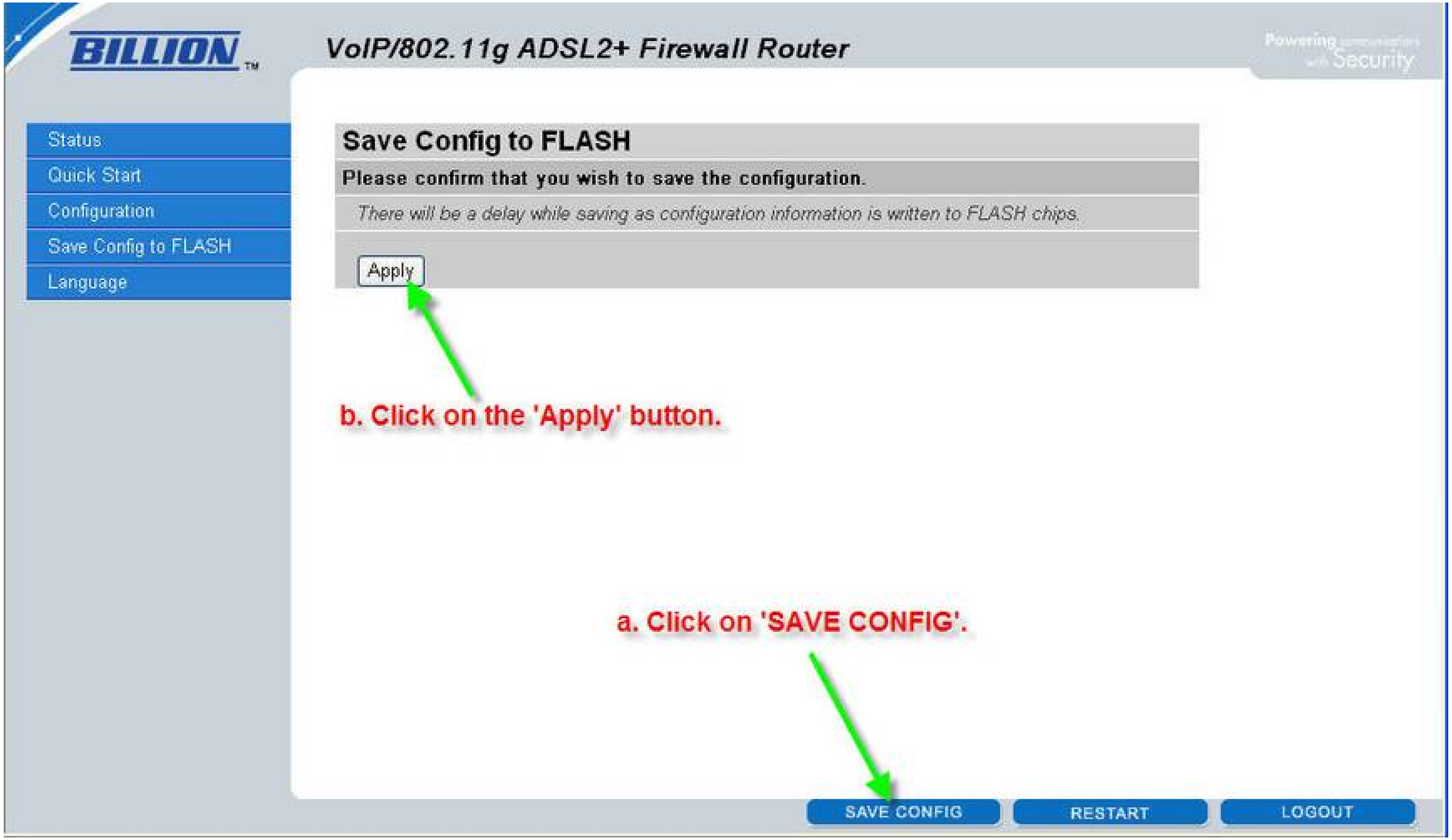
12. Internal ports

13. 'Allow' or 'Block' inbound traffics.

14. 'Allow' or 'Block' outbound traffics.

15. Click on the 'Apply' button.

After the settings are applied you must save the setting permanently.



Save Config to FLASH

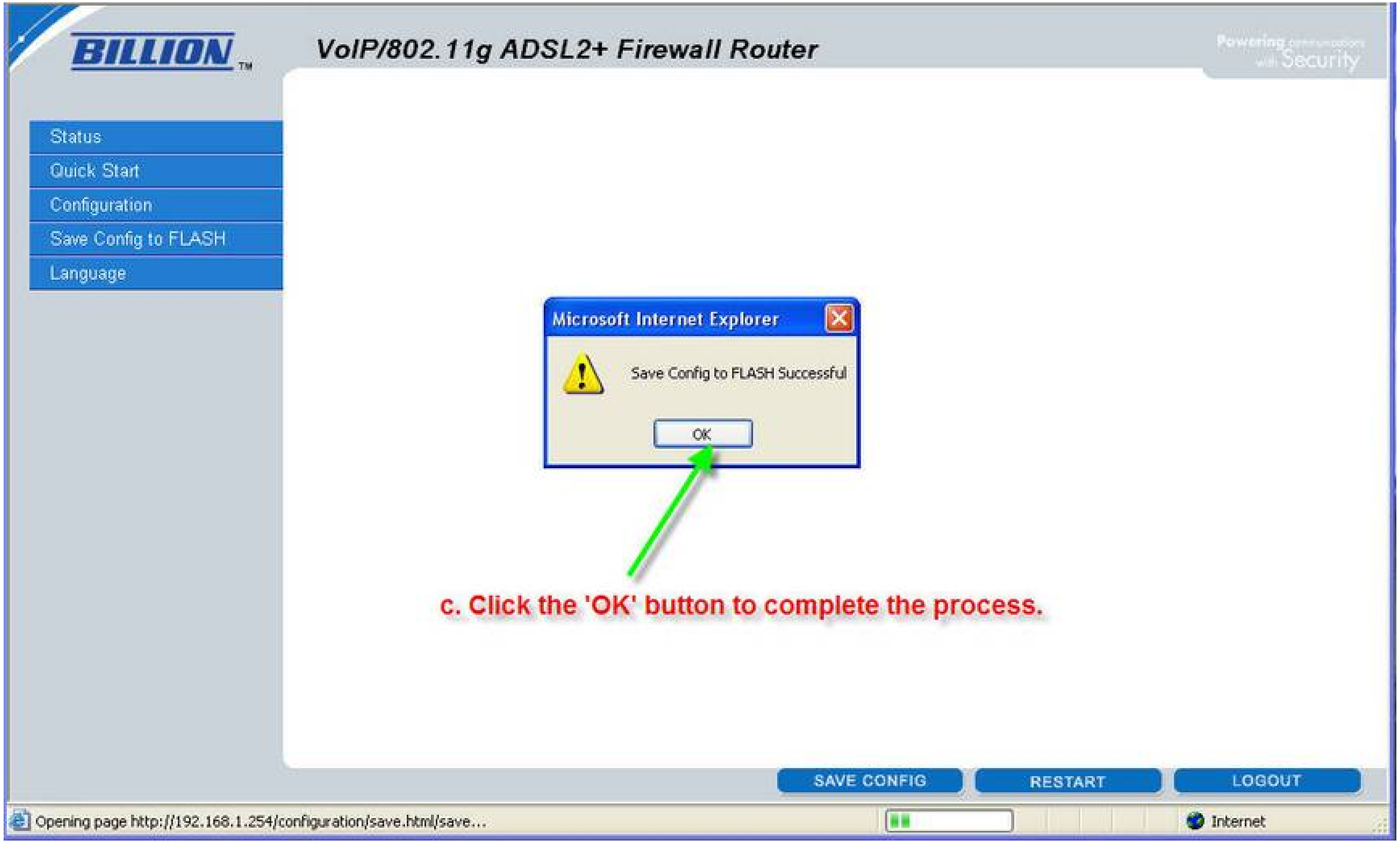
Please confirm that you wish to save the configuration.

There will be a delay while saving as configuration information is written to FLASH chips.

Apply

b. Click on the 'Apply' button.

a. Click on 'SAVE CONFIG'.


BILLION
VoIP/802.11g ADSL2+ Firewall Router
Powering communications with Security
Status
Quick Start
Configuration
Save Config to FLASH
Language
Microsoft Internet Explorer
OK
SAVE CONFIG
RESTART
LOGOUT
Internet

Save Config to FLASH Successful

c. Click the 'OK' button to complete the process.

Opening page http://192.168.1.254/configuration/save.html/save...