### **Configuring the Firewall**

Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including:

- IP Spoofing
- SYN flood
- Land Attack
- UDP flooding
- Ping of Death (PoD)
- Tear Drop Attack
- Denial of Service (DoS)
- ICMP defect
- IP with zero length
- RIP defect
- Smurf Attack
- Fragment flooding
- TCP Null Scan

The firewall also masks common ports that are frequently used to attack networks. These ports appear to be "stealth", meaning that for all intents and purposes, they do not exist to a would-be hacker. You can turn the firewall function off if needed; however, it is recommended that you leave the firewall enabled. Disabling the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you leave the firewall enabled.

Firewall >
Your Router is equipped with a firewall that will protect your network from a wide array of common hacker attacks including Ping of Death (PoD) and Denial of Service (DoS) attacks. You can turn the firewall function off if needed. Turning off the firewall protection will not leave your network completely vulnerable to hacker attacks, but it is recommended that you turn the firewall on whenever possible.
Firewall Enable / Disable > C Disable @ Enable
Clear Changes Apply Changes

# **Configuring Internal Forwarding Settings**

The Virtual Servers function will allow you to route external (Internet) calls for services such as a web server (port 80), FTP server (Port 21), or other applications through your Router to your internal network. Since your internal computers are protected by a firewall, computers outside your network (over the Internet) cannot get to them because they cannot be "seen". A list of common applications has been provided in case you need to configure the Virtual Server function for a specific application. If your application is not listed, you will need to contact the application vendor to find out which port settings you need.

BEEKIN					Homei Helni Lo	nout Internet Statue: Comm
LAN Setup					nome; nep; co	jour internet stutus, citrin
LAN Settings	Fire	wall > Vir	tual servers			
DHCP Client List						
Internet WAN	This function will allow you to route external (Internet) calls for services such as a web server (nort 80) FTP server (Port 21) or other applications through your Router to your internal					
Connection Type	1	network. M	tore Info			
DNS						
MAC Address			Clear Cha	nges	Apply Changes	
Wireless Super A			Add Active Worlds		▼ Add	
Channel and SSID			lear entry		Clear	
Security	1.0	-				
Wireless Super G		Enable	Description	Туре	Private IP address	Private port
Channel and SSID	1.			TCP -	192.168.2	
Firewall						
Virtual Servers	2.			TCP 🗾	192.168.2.	
Client IP Filters		_		TOD H		
DMZ	3.			TICP •	192.168.2.	
WAN Ping Blooking	4.			TCP -	192,168,2	
Security Log						
Utilities	5.			TCP 🗾	192.168.2.	
Use as Access Point		-				
Parental Control	0.	-		True M	192.168.2.	
Restart Kouter	7.			TCP -	192.168.2.	
Sava@ackup Sattings	_					
Restore Previous Settings	8.			TOP -	192.168.2.	
Firmware Update		-		TCD -		
System Settings	9.			pros 🖻	192.168.2.	
	10.			TCP .	192 168 2	

# **Choosing an Application**

Select your application from the drop-down list. Click "Add". The settings will be transferred to the next available space in the screen. Click "Apply Changes" to save the setting for that application. To remove an application, select the number of the row that you want to remove then click "Clear".

# Manually Entering Settings into the Virtual Server

To manually enter settings, enter the IP address in the space provided for the internal (server) machine, the port(s) required to pass (use a comma between multiple ports), and then select the port type (TCP or UDP) and click "Apply Changes". You can only pass one port per internal IP address. Opening ports in your firewall can pose a security risk. You can enable and disable settings very quickly. It is recommended that you disable the settings when you are not using a specific application. 9

## Setting Client IP Filters

The Router can be configured to restrict access to the Internet, email, or other network services at specific days and times. Restriction can be set for a single computer, a range of computers, or multiple computers.



To restrict Internet access to a single computer, for example, enter the IP address of the computer you wish to restrict access to in the IP fields (1). Next, enter "80" in both the port fields (2). Select "Both" (3). Select "Block" (4). You can also select "Always" to block access all of the time. Select the day to start on top (5), the time to start on top (6), the day to end on the bottom (7), and the time to stop (8) on the bottom. Select "Enable" (9). Click "Apply Changes". The computer at the IP address you specified will now be blocked from Internet access at the times you specified.

**Note:** Be sure you have selected the correct time zone under "Utilities> System Settings> Time Zone".



#### Enabling the Demilitarized Zone (DMZ)

The DMZ feature allows you to specify one computer on your network to be placed outside of the firewall. This may be necessary if the firewall is causing problems with an application such as a game or video conferencing application. Use this feature on a temporary basis. The computer in the DMZ is NOT protected from hacker attacks.



To put a computer in the DMZ, enter the last digits of its IP address in the IP field and select "Enable". Click "Apply Changes" for the change to take effect. If you are using multiple static WAN IP addresses, it is possible to select which WAN IP address the DMZ host will be directed to. Type in the WAN IP address you wish the DMZ host to direct to, enter the last two digits of the IP address of the DMZ host computer, select "Enable" and click "Apply Changes".

#### **Blocking an ICMP Ping**

Computer hackers use what is known as "pinging" to find potential victims on the Internet. By pinging a specific IP address and receiving a response from the IP address, a hacker can determine that something of interest might be there. The Router can be set up so it will not respond to an ICMP ping from the outside. This heightens your Router's security level.

Firew	all > WAN Ping Blocking	
ADVAN port). T	CED FEATUREI You can configure the Router not to respond to an ICMP Ping (ping to the WAN his offers a heightened level of security. More Info	
	Block ICMP Ping > V	_ (1)
	Clear Changes Apply Changes	

To turn off the ping response, select "Block ICMP Ping" **(1)** and click "Apply Changes". The Router will not respond to an ICMP ping.

# Utilities

The "Utilities" screen lets you manage different parameters of the Router and perform certain administrative functions.

#### **Parental Control**

See the included Parental Control User Manual for more information on the Parental Control feature.

#### **Restarting the Router**

Sometimes it may be necessary to restart or reboot the Router if it begins working improperly. Restarting or rebooting the Router will NOT delete any of your configuration settings.

# Restarting the Router to Restore Normal Operation

1. Click the "Restart Router" button.



2. The following message will appear. Click "OK".



3. The following message will appear. Restarting the Router can take up to 60 seconds. It is important not to turn off the power to the Router during the restart.



4. A 60-second countdown will appear on the screen. When the countdown reaches zero, the Router will be restarted. The Router home page should appear automatically. If not, type in the Router's address (default = 192.168.2.1) into the navigation bar of your browser.

# Using the Web-Based Advanced User Interface

# Restoring Factory Default Settings

Using this option will restore all of the settings in the Router to the factory (default) settings. It is recommended that you back up your settings before you restore all of the defaults.

Restore factory defaults

Litilities > Restore Factory Defaults

- 1 Click the "Restore Defaults" button
- 2. The following message will appear. Click "OK".

- 3. The following message will appear. Restoring the defaults includes restarting the Router. It can take up to 60 seconds. It is important not to turn the power to the Router off during the restart.
- 4. A 60-second countdown will appear on the screen. When the countdown reaches zero, the Router's defaults will be restored. The Router home page should appear automatically. If it does not, type in the Router's address (default = 192,168,2,1) into the navigation bar of your browser.







sing this option will restore all of the settings in the Router to the factory (default) settings. It is commended that you backup your settings before you restore all of the defaults. To restore th chorv default settings, click the "testore Defaults" button below.

### Saving a Current Configuration

You can save your current configuration by using this feature. Saving your configuration will allow you to restore it later if your settings are lost or changed. It is recommended that you back up your current configuration before performing a firmware update.



 Click "Save". A window called "File Download" will open. Click "Save".

File Dov	vnload 🛛 🔀
?	You are downloading the file: config.bin from 192.168.2.1
	Would you like to open the file or save it to your computer?  Open Save Cance More Info Always ask before opening this type of file

2. A window will open that allows you to select the location where vou want to save the configuration file Select a location You can name the file anything you want. or use the default name "Config". Be sure to name the file so you can locate it yourself later. When you have selected the location and name of the file. click "Save".



 When the save is complete, you will see the following window. Click "Close".

The configuration is now saved.

Download complete
Download Complete Saved: config.bin from 192.168.2.1
Downloaded:         16.0 KB in 1 sec           Download to:         C1/Documents and Setting (config.bin           Transfer rate:         16.0 KB/sec           Close this dialog box when download completes         0

# **Restoring a Previous Configuration**

This option will allow you to restore a previously saved configuration.

nusly saved configuration.
Browse

1. Click "Browse". A window will open that allows you to select the location of the configuration file. All configuration files end with a ".bin". Locate the configuration file you want to restore and double-click on it.

Choose file		? 🔀
Look in: My Recent Documents Desktop My Documents My Computer	Desktop      Desktop	
My Network Places	File name: config  Files of type: All Files (".")	Open Cancel

2. You will be asked if you want to continue. Click "OK".



**3.** A reminder window will appear. It will take up to 60 seconds for the configuration restoration to complete. Click "OK".



**4.** A 60-second countdown will appear on the screen. When the countdown reaches zero, the Router's configuration will be restored. The Router home page should appear automatically. If not, type in the Router's address (default = 192.168.2.1) into the navigation bar of your browser.

### Updating the Firmware

From time to time, Belkin may release new versions of the Router's firmware. Firmware updates contain feature improvements and fixes to problems that may exist. When Belkin releases new firmware, you can download the firmware from the Belkin update website and update your Router's firmware to the latest version.

Firmware Update		
From time to time, Belkin may updates contain improvements below to see if there is a new f NOTE: Please backup your cun Click Here to go to the Saveß	release new versions of the Router's firmware. Firmware and fixes to problems that may have existed. Click the link irmware update available for this Router. rent settings before updating to a new version of firmware. ackup current settings page.	(1
Check For New Firmware Version	Check Firmware	
Update Firmware >	Update	

### Checking for a New Version of Firmware

The "Check Firmware" **(1)** button allows you to instantly check for a new version of firmware. When you click the button, a new browser window will appear informing you that either no new firmware is available or that there is a new version available. If a new version is available, you will have the option to download it.

#### Downloading a New Version of Firmware

If you click the "Check Firmware" button and a new version of firmware is available, you will see a screen similar to the one below.



- 1. To download the new version of firmware, click "Download".
- 2. A window will open that allows you to select the location where you want to save the firmware file. Select a location. You can name the file anything you want, or use the default name. Be sure to save the file in a place where you can locate it yourself later. Note: We suggest saving this to your desktop to locate the file easily. When you have selected the location, click "Save".



**3.** When the save is complete, you will see the following window. Click "Close".



The download of the firmware is complete. To update the firmware, follow the next steps in "Updating the Router's Firmware".

# Updating the Router's Firmware

- In the "Firmware Update" page, click "Browse" (2). A window will open that allows you to select the location of the firmware update file.
- 2. Browse to the firmware file you downloaded. Select the file by double-clicking on the file name.



3. The "Update Firmware" box will now display the location and name of the firmware file you just selected. Click "Update".

Utilities > Firmware Update	
From time to time, Belkin may release ne contain improvements and fixes to proble is a new firmware update available for th	w versions of the Router's firmware. Firmware updates ms that may have existed. Click the link below to see if there is Router.
NOTE: Please backup your current setting to go to the Save/Backup current setting	is before updating to a new version of firmware. Click Here page.
Check For New Firmware Version >	Check Firmware
Update Firmware >	Browse
	Update

4. You will be asked if you are sure you want to continue. Click "OK".



5. You will see one more message. This message tells you that the Router may not respond for as long as one minute as the firmware is loaded into the Router and the Router is rebooted. Click "OK".



**6.** A 60-second countdown will appear on the screen. When the countdown reaches zero, the Router firmware update will be complete. The Router home page should appear automatically. If not, type in the Router's address (default = 192.168.2.1) into the navigation bar of your browser.