FireBrick User Guide

Andrews & Arnold/Watchfront

Table of Contents

Table of Contents

Table of Contents

FireBrick User Guide

This User Guide is intended to provide a basic introduction to the operation of the FireBrick. The full Technical Reference Manual is also available to answer detailed questions about its operation.

More information about the FireBrick generally can be found at http://www.FireBrick.co.uk/

FireBrick is a registered trademark of Andrews &Arnold Ltd and Watchfront Ltd.
Copyright © 2000/2001 Andrews &Arnold/Watchfront

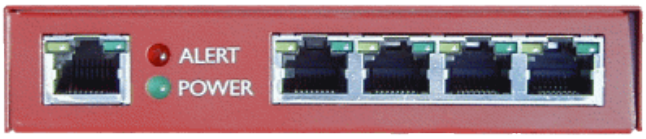
Issue 1.6, 14 May 2001

Getting Started

Sockets and connectors The FireBrick® has 7 sockets and 12 LEDs.

On the rear is the power connector for use with the power supply provided. This is intended for use indoors on a normal UK mains supply, and can be connected to an uninterruptable power supply (UPS) if required. Power connectors for use outside the UK may be obtained from your distributor.

Also on the rear is a 9−way D serial connector. This is for factory test and future development, so does not normally need anything connected.



On the front there is a single network socket on the left. This is the connection to the outside world − the Wide Area Network (WAN). It is designed to connect to a hub using a normal network patch lead. The term WAN is used throughout this manual and the software configuration pages. It is possible to use the FireBrick® in other configurations, but the term WAN is always used to refer to this left hand single network socket.

On the right are four network sockets. These are for your Local Area Network (LAN) and connect your computers or other hubs to the FireBrick®. These are a hub and are designed to connect to computers using a normal network patch lead. If you are connecting another hub to any of the LAN sockets you will either need a *crossover* lead or you will need to use the *uplink* socket or setting on the hub to which you are connecting. The term LAN is used throughout this manual to mean the 4 network sockets on the right.

Lights

If you power up the FireBrick® with no network connections then the green power light will be lit, and the eight LAN lights will cycle right and left continually. This is an indication that the FireBrick® is working correctly and waiting for network connections on its LAN. Once the LAN is correctly connected the lights will stop cycling.

The green power light will be on when the FireBrick® is plugged in to the power. If this blinks continually then the FireBrick® is faulty.

The red alert light is used for several functions. It blinks momentarily on power up to show it is working, and will blink rapidly while you upgrade the software. Normally this light is off unless you have set a network filter to make it flash − e.g. when there is a certain type of access to your network. You can configure certain network filters to make this light blink slowly all of the time until you clear it.

Above each network socket are two lights. The LAN lights can be changed to operate in different modes, but normally the LAN and WAN lights operate in the same way, as follows:

- The green light on the right indicates that there is a good connection to another network port − e.g. a hub or computer is correctly connected. If you are using the wrong sort of cable or the cable is faulty or the other end is not switched on or is the wrong type of network port then the green light will not be lit.
- The yellow light on the left indicates network activity. This means there is data being received by that port.

The network lights on the LAN can be configured with different settings including a network bar graph showing overall LAN usage, and a cycling lights option even when there are network connections active.

Connecting to your network

The FireBrick® is designed to fit in−line with an existing network connection. This means that you connect the WAN side of the FireBrick® to an existing router or network hub, and the LAN side to your computer(s) or hubs.

If you are already connected to a router, network hub, or floor box, remove the existing cable from the router/hub/box and connect it to any of the LAN ports on the right of the FireBrick®. The green light above the socket on the FireBrick® will light.

Then connect the patch lead supplied from the WAN port on the FireBrick® to the existing router, network hub, or floor box. Again the green light above the WAN socket on the FireBrick® will light.

You may also see the yellow lights above each port light as data is sent and received on the network.

You can normally connect and remove network plugs without disconnecting the power from computers, hubs, or the FireBrick® without any problem.

The only complication can be where your existing router is not itself a hub, and so uses a crossover lead or connects to a crossover port on a hub. In this case you may need to connect the FireBrick® and the existing router to a separate hub, or use a crossover lead to connect the FireBrick® to the existing router. Crossover leads can be purchased from your dealer. As long as the green light is lit over each of the cables you connect the FireBrick® is correctly cabled.

Hubs and networks

The FireBrick® is designed to operate on a 10baseT network connection. This means that it uses the 8−way RJ45 connectors which fit in the front and operates at 10,000,000 bits per second.

Some networks use 100baseT which operate 10 times faster. Normally such networks use *switching hubs* which allow a mixture of 10baseT and 100baseT systems to be connected, automatically adapting. Some hubs have lights indicating that they are operating in 10baseT or 100baseT on each port. Most computers that use 100baseT will also automatically adapt to 10baseT.

10baseT networks can manage a 2Mb/s internet connection (that's 2,000,000 bits per second each way, making 4Mb/s total) without much problem. Remember that 10Mb refers to the raw data rate on the network, and not the maximum speed that you could transfer files (which is much lower).

If you connect the FireBrick® to a network hub or computer that can only operate at 100baseT the green light will not come on, but it will not do any harm to the FireBrick® or the computer/hub. In such cases you can purchase small 10/100 switching boxes relatively cheaply that would allow you to connect the FireBrick®.

If you needed to take a fast (say 34Mb/s) internet feed and split it down to several small offices (e.g. a managed office or hotel situation), then you can use a 10/100 fully switching hub and a bank of FireBrick®s to provide each office with up to 2Mb of internet connection.

Some networks operate using 10base2 which uses round (coax) connectors. The FireBrick® will not connect to these directly but you can buy a cheap network hub that will allow you to connect 10baseT and 10base2 networks together.

Some routers already have a 4−port hub, and you may have several cables already connected. These should all be moved to the FireBrick® LAN ports and a single cable from the FireBrick® WAN port connected to one of the sockets on the router. If you connect anything else to the spare sockets on your router then they will be outside your firewall and not protected by the FireBrick®.

Checking all is well

Once you have connected the FireBrick® between your computer(s) and your internet connection, you should check your system is still working. The simplest way to do this is to access a web page (such as http://www.FireBrick.co.uk/) and check that it displays correctly. Use *refresh* to make sure you are loading the page from the server and not a locally cached copy.

Configuration pages

Once the FireBrick® is connected and you have working internet access you can access the FireBrick® configuration pages using your web browser to access http://my.FireBrick.co.uk/. This will bring up a red screen with the FireBrick® logo in the top right. If, instead, you see a different page with *this is not your FireBrick®* then this means your FireBrick® has not intercepted the *my.FireBrick.co.uk* address. This could be because you are accessing the internet by another means, or the FireBrick® is not connected correctly, or you are *behind* the FireBrick®. To access the FireBrick® configuration pages you need to ensure you are not using a proxy. You can either turn off your proxy settings in your web browser or list *my.FireBrick.co.uk* as a *no proxy* site and try again. If this fails, use the *standalone configuration* as below. Also, try using the refresh/reload button on your browser, and try with SHIFT or CTRL keys as well, ad you browser may have cached a copy of the *this is not your FireBrick®* page from some time before.

Standalone configuration

So far we have assumed you have an existing ethernet network connection in to which the FireBrick® can be inserted. If however you do not have such a network connection, or you want to configure the FireBrick® and familiarize yourself with its operation before unplugging your network, then you will need to access the FireBrick® in standalone mode.

To do this you will need a computer with a web browser on which you can change the network settings. On Windows select *Network* on the Control Panel, choose the *Protocol* tab, highlight *TCP/IP Protocol* and click *properties*. Set your computer to have IP address 217.169.0.2 and a netmask of 255.255.255.252. You do not need to set or change your DNS, WINS, or gateway settings. You may have to reboot your computer for these changes to take effect.

An alternative is to add a network route. On windows, do this in Start−>Run with the command **ROUTE ADD 217.169.0.1 *yourIP***. On linux the command is **route add −host 217.169.0.1 eth0**. You should then be able to access the web page as below.

Then, using your web browser, and ensuring you have no proxy settings, access the FireBrick® configuration pages using http://217.169.0.1/. This will provide the same web configuration page, and you will be able to set up the FireBrick® as you require.

DHCP startup

You can factory reset the FireBrick® such that it is running a DHCP server, thus allowing you to set your PC to automatic IP configuration. To do this, disconnect all network cables and power. Then, connect a straight network cable (as supplied) in from the WAN (left) to one of the LAN ports and then reconnect the power. After a second the red LED lights, and you can remove the network lead. The FireBrick® will reset with a DHCP mode depending on which of the hub ports you connected the cable to as follows:−

Hub port	Factory reset operation
0 (left)	DHCP server on LAN and DHCP client on WAN
1	DHCP server on LAN
2	DHCP client on WAN
3 (right)	Normal, non DHCP mode

Having selected DHCP on the LAN, you can connect a PC set to automatic IP allocation, and access the FireBrick using http://217.169.0.1/.

Brick walls

If you have lots of FireBrick®s, they can be stacked on top of each other. The rubber feet fit in to the dimples on the top.

What's protected

Installing a FireBrick® will provide instant protection from the internet, but what does this mean...

Firstly, you can still access the internet. The FireBrick® allows all outgoing traffic (apart from NETBIOS file shares) to go out in to the world. This means you can access web pages and send email, etc. The FireBrick® automatically tracks information which is a reply to those outgoing connections and lets it back in.

The FireBrick® blocks all other incoming traffic. There are however a number of filters predefined that can easily be turned on to allow, for example, incoming SMTP mail delivery.

FAQ

This document includes answers to frequently asked questions, as well as general tips.

I can only see Setup and Users menus, shouldn't there be more?

Out of the box the FireBrick does not require any login to access the basic settings. In this state most of the menus are hidden.

You should set up an admin user, and log in as the admin user. This makes the FireBrick much more secure and allows you to see all of the menus.

To do this, go to users, select admin, and enter a password (in both boxes) and save. Then select login from the top left and enter the username admin and the password you chose. You should then see more icons and menus. You can then go to users, select nobody, and un−tick the view and edit rights for level 1 and save. In future, always log in. You can change the user name from admin to something else if you wish, and add others users.

I cannot access the FireBrick any more − HELP!

The FireBrick has a lot of security, and it is quite easy to configure yourself in to a hole − not allowing you access. There are default filters to stop you doing this by mistake, and it is wise to leave these in place and active until you are sure what you are doing. It is also wise to save the config regularly, so that if you have to factory reset the FireBrick, you can go back to the last working state and not have to start again. If you have managed to make such a configuration, or even simply forgotten your password, then the only option is a factory reset.

To factory reset your FireBrick, remove all connections from it, and then use a straight patch lead (as supplied) to connect the WAN (left hand) port to the far right hand LAN port. Then power up and wait a second for the red light to come on. Then remove the patch lead. The FireBrick will blink its lights then go show cycling lights − it is now factory reset.

I have set the user to WAN access, but it just says "Goodbye"

So you want access from outside ? You must also set the nobody user to WAN access, as this is required to show the log in screen at all.

I cannot set the clock!

The clock is set from the internet, but to do this the FireBrick must be able to talk to the internet. This is normally via the WAN port to the time servers configured in the FireBrick by default. Just because you can talk to the internet from a PC on your LAN via the FireBrick does not mean the FireBrick knows how to − this is the case in stealth mode.

To get packets to the internet, the FireBrick will need two key things − a gateway, and an IP address. The gateway is just the address of your router on the WAN side and is set in the setup menu. The IP address is a different matter − it can either be a public IP address set up using a subnet on the WAN side, or can be a stealth address. Either way it must be an address which will

find its way back to the FireBrick from the time servers on the internet.

If you do not want to give your FireBrick its own address, then it can *borrow* one from your LAN. In the setup/stealth menu set the WAN stealth address (previously blank) to the public address of a machine on your LAN which is normally switched on. The FireBrick can then borrow this address to set the clock. This should have no effect on the operation of that machine. Don't change the LAN stealth address (normally 217.169.0.1).

Normally after a change in config, the clock is set, but you can force it by selecting the Set button in the clock setting menu under setup. If the clock is set for the first time and you are logged in, you will probably find you are logged out.

I cannot get FTP to work

The way FTP works means that it normally tries to make a separate connection back to you when you try to transfer a file or view a directory. This connection is quite separate and is seen by the FireBrick as an unwanted incoming connection.

There are two possible problems with this − firstly that you will quite sensibly have filtering stopping such unwanted incoming connections. You can get around this, reducing your security, by allowing some traffic in. You should restrict the IP addresses if possible, e.g. if it is your web server you are FTPing to − allowing connections only from that FTP server. Also, only allow connections to ports 1024 to 65535. If you look at your logs you may find that the incoming connections only come from a specific port, such as port 20 or 21, and this can make the filter even more specific. The other solution is to use passive mode (see below).

The other problem is with NAT − i.e. you have a private address, and the FireBrick is converting this to a real address for you. The FTP control session tells the other end to connect back to a specific place and port, but if you are on a private address block, it will tell the other end to connect back to a non existent address and it won't work. The only way around this is to use passive mode.

Passive mode simply means that instead of the other end connecting back to your FTP client when you transfer data, you connect to the FTP server again. This solves most problems, but not all FTP clients have a passive mode. It is recommended that you use a client that does have a passive mode (it may also be called a firewall mode).

You will however be unable to use passive mode where the ftp server at the far end also has a firewall, simply because it will not allow your extra connections to the FTP server. This is simply one of the downsides of having some security.

I have set port mapping to one of my other public addresses but it does not work

Typically, if you have a small block of public addresses, with the FireBrick on one of them, and you want to set port mapping of some of the other public addresses you have through to machines on your LAN. You set up the port map on the FireBrick, and ensure the filters are allowing traffic, but it still does not work and nothing appears in the log even...

This is an ARP issue. The internet router expects the other public addresses to be on the ethernet (WAN) and tries to ARP for them. This gets no reply, and so the router does not even try to send the packet (hence no log entry on the FireBrick).

To solve this you need to make the FireBrick ARP reply for these other addresses. This can be done in one of two ways.

1. Add additional WAN subnets quoting the IP addresses you want the FireBrick to answer on.
2. Add a route from WAN to LAN for a range of public addresses, marked "Proxy ARP"

Either way the packets will get to the FireBrick, and so should work. Check logs for any clues to missing filters that you may need.

I think filters are getting in the way

Basically, if you set up anything complex, such as port mapping, complicated routing, or tunnels, you can be caught out by filters. It is important to realise that filters are checked in order − so an early filter may block traffic which you allow in a later filter.

A good tip to eliminate filters to to move a filter to the top of the list that is Any−>Any with everything blank, Allow, and Log. If what you are doing works in this situation, the problem was filters and you can check the log to see what is happening. Pay attention to the interfaces (WAN/LAN/Tunnel, etc) and IPs and ports of the sessions being allowed by the filter, and set up filters to allow the traffic you require.

When you have finished remove or suspend the Any−>Any filter to ensure you are firewalled again.

Basic Filtering

The main FireBrick® configuration pages provide a list of filters which you can control.

The list is in three sections − traffic allowed in to your network, traffic allowed out of your network, and other.

Each item in the filter list is either allowed (shown in green) or ignored (shown in red), and can be changed using the checkbox next to the item and pressing the *Update quick firewall settings* button. It's that simple!

Filters that are ignored will result in the packets being dropped, as this is the *default filter* action.

Internet traffic operates on three basic protocols, two of which have port numbers. Specific applications on the internet will use one of these protocols and one or more ports. For example web pages normally work on TCP port 80. Port numbers under 1024 are normally called privileged ports. Many network services are on these ports including web pages, email, news, etc.

It is important to realize that the filters operate in order and work on the first match found. Filters which are being ignored (suspended) are skipped over, but the first filter which matches will apply, whether it allows or drops the traffic.

You will notice that initially there is no login or security check to allow you to set the basic filtering. This is to make it simple and easy to use. By default it is only possible to get to this configuration page from the inside of your network (the LAN ports). You should, however, consider setting up login security on your FireBrick®. Once you have done this you can still allow some settings to be changed if you wish, but you can configure which settings are available on the main screen.

User Security

Out of the box the FireBrick® allows access from the local network (LAN ports) to set basic filters and change configuration. This makes the basic operation of the FireBrick® very simple, but even restricting the operation to the LAN this does not make it very secure in a larger office.

You should therefore consider setting up user security on your FireBrick®. You must be careful when doing this as it is quite possible to lock yourself out completely (see Don't Panic).

Basic security model

The FireBrick® uses a basic user login security model. When you access the FireBrick® web pages you are initially the *nobody* user. This is a user like any other, but has no password. You can control what the access that the *nobody* user has. All other users require a login using a username and password.

Each user has a set of up to 8 security rights. These allow *view* or *edit* at each security level. The most powerful user would have view and edit for all security levels 1 to 8. By default, the *nobody* user has rights for level 1 view and edit only.

Each of the settings in the system then has a security level (1−8). Only if you have view access at a specific level can you view those settings. Similarly, only if you have edit rights at that level can you change a setting.

Creating the admin user

In order to set up other users you will need to set up an all powerful admin user. Select the *Users* icon from the top of the page and select the *admin* user that is already set up. You can then enter a password (enter it twice) and save the settings.

Once you have done this you can log in as the admin user using the *login* link on the top left of the page. Enter the username and password carefully. Once logged in the name is shown on the top left and a *Logout* link. If this does not work, go back and check the password on the user settings is correct and try again.

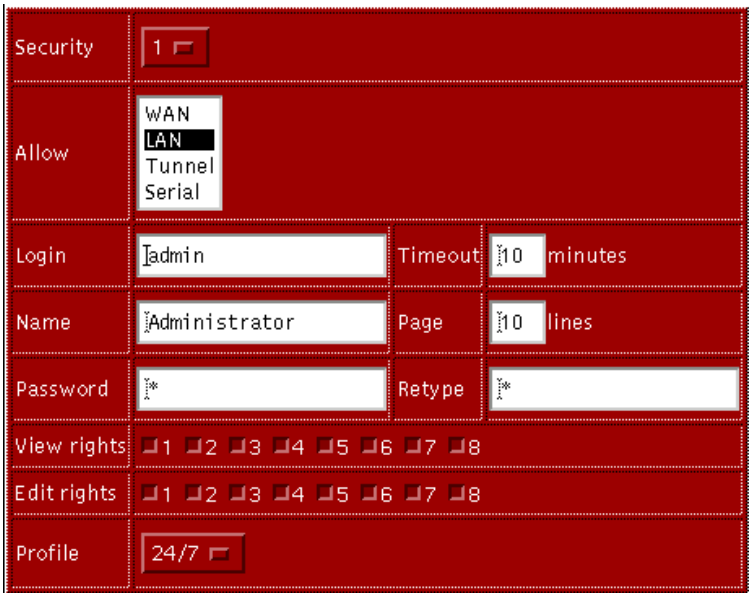
Stopping general access

If you want to stop general access to the FireBrick®, all you have to do is restrict the permissions of the *nobody* user. Don't do this until you are sure you have managed to log in as the *admin* user! Simply edit the *nobody* user and change the view/edit settings so that there is no view or edit access at any level.

This will have the effect that the main login screen, when not logged in, will now be blank rather than listing a set of filters. This is because these filters are all level 1 security and the *nobody* user no longer has that access. You could obviously leave the *nobody* user at level 1 access and change all other settings to be a level other than 1. You could decide that you will make level 8 the *low security* setting and make the *nobody* user level 8 edit and view and then only set specific entries to level 8 security. The level numbers do not have a specific meaning, so 8 is not a *higher security setting* than 1.

User settings

The basic user settings are as follows :−



Security	Controls the level of security of this entry, restricting who can view and change the user
Allow	Where the user can log in from
Login	The login name
Timeout	The auto logout timeout in minutes
Name	The full name of the user
Page	The number of lines shown on each page of multi page configurations
Password	The password − enter twice to be sure
View rights	Which security levels the user can view
Edit rights	Which security levels the user can edit
Profile	The profile (e.g. time of day) when the user is allowed to log in

General access

The main setup page contains a list of security settings that affect general aspects of the FireBrick®. These include security settings for access to each of the main configuration pages as well as software upgrade ability. Ensure that these are set to fit in with your user security scheme. Care should be taken with the upload/save config level a this allows a complete configuration to be saved or replaced.

Access from outside

You will only be able to access the FireBrick® from outside if you have configured a suitable IP address. By default no access is permitted to the configuration pages from the WAN, so you will need to make a number of changes to allow remote access :−

- Enabled the FireBrick−remote filter which allows access WAN−>FireBrick for TCP port 80
- Change the nobody user to have WAN access − allows access to the login pages

- Change the required user(s) to have WAN access − allowing the loging from outside.
- Also ensure that the nobody user has no rights to do anything

Always consider security carefully. Test what you have done wherever possible − i.e. try logging in from outside and from where you should not be able to.

Always ensure you have a valid login yourself before making changes you are unsure about. You may even want to set up a separate backup admin login with a very obscure password just in case you lock yourself out. If in doubt, save the configuration before a change.

Controlling access

A typical situation may be that you wish to control access. i.e. you want certain specific settings on the FireBrick® that you have set, and want to allow someone else to be able to make some additional changes. For example you may want certain filters, but allow someone else to add extra filters.

This can be done by setting the appropriate security levels on the user and on the settings you want to control. You can choose if the user will be able to see the settings you have fixed or not.

If you do this, you must be careful to consider the order in which settings apply. For example, filters are applied in order. So your *fixed* settings must be first in the list otherwise they could be overridden by something your user can change.

As an example, a managed office may want to impose speed limiting controls yet allow the tenants to set up the firewall filters. This allows responsibility for filtering to be given to the tenants but stops them being able to override some basic settings such as the speed of their access.

Simple settings

There are a number of one−off simple settings in the main setup page.

Save config

This allows to you save the configuration to your local hard disk. Click on this and your browser should give you the option of a filename to save the file to. You will only be able to save if you have the appropriate security level.

Note that saving the config also clears the log.

Upload

You can upload new software or saved configuration files using this option. Uploading a configuration will replace the existing configuration, and is only available if you have the appropriate security level.

To upgrade the FireBrick® you must first download the software file(s) from http://software.FireBrick.co.uk/ and store these on your computer. You can then select the upload option and select the file to upgrade your FireBrick®. The upgrade process can take up to a minute during which time the red light will flash rapidly and all of the LAN hub lights will flash. When they stop the FireBrick® is upgraded.

You must not interrupt the power during the upgrade. If you do you could end up with a dead FireBrick® (see Don't Panic).

An upgrade will not normally change your configuration or reset statistics or DHCP tables, but this depends on the versions you are using. Always check your configuration carefully after an upgrade. It is usually a good idea to save your config before upgrading, as downgrading later may not preserve your config fully.

Once the main (F) file is loaded, you will need to load the user interface file (e.g. WEN for English). WIthout this the FireBrick® still operates, but cannot be configured.

Note that uploading also clears the log.

Clear Alert

This is only shown if the red light is slowly flashing, meaning an alert has been set by the filtering rules. Click on the link to stop the light flashing. If the clock is set, then the date and time of the alert is also shown.

Hub LEDs

This setting allows you to control the meaning of the yellow and green lights on the four LAN ports. Various options allow the status of the network connection to be displayed in different ways. The default is setting 2 which shows activity and link status in the same way as the WAN lights.

Options include a bar graph mode which uses the 8 lights as a usage level indicator − lighting more lights from the left. When in a wall of FireBrick®s this allows network usage per FireBrick® to be

seen at a glance.

Another option is a cycling lights option. Note that selecting this does cause a harmless local network packet to be sent on the WAN connection every 1.5 seconds, which would not go out to the internet. If you have a wall of FireBrick®s you can select cycling lights on all of them at once and you will be able to see what this network packet is used for...

Name

You can name your FireBrick®! If you have to administer several FireBrick®s then it is sensible to name each one so that you can see at a glance which one your are configuring. The name appears at the top of the screen along with the serial number. You can also supply a Domain which is used by DHCP.

Gateway

When deciding where to send a packet of data the FireBrick® first checks the routing rules, then the local subnets and finally the default gateway route. Set this to the address of your main gateway to the internet. This is normally the IP address of your router.

The gateway only affects routed traffic, and not stealth traffic, so if it is not set the FireBrick® will work in stealth mode and will only communicate with local networks. It is important to set the gateway address when the FireBrick® is being used as a router (with or without NAT) and is treated as a gateway itself by local computers. It is also important to set this when the FireBrick® needs to know the time of day itself and the time server is on an external machine (as it will be if the default time server is used).

If the FireBrick® is a DHCP client on the specified interface then the gateway is normally set automatically. To remove the gateway, set the address to 0.

Stealth IP

The FireBrick® configuration pages work on the web page http://my.FireBrick.co.uk/ or the IP address 217.169.0.1. This is a real internet address which we have reserved for the purpose. When accessing the FireBrick® configuration pages the FireBrick® intercepts the access to this address. It effectively *borrows* this address for its own use.

You can change the address that is intercepted, but it is unlikely you will ever need to. If you have given your FireBrick® a real IP address then you may not want to allow any interception, in which case set this address to 0. Please test access to the configuration pages using a real IP address before you do this as you might otherwise be completely locked out (see Don't Panic).

You can also set an address for the WAN stealth operation. This is an address that the FireBrick® borrows for things it sends to the internet itself, such as time requests. It is only necessary if you are not giving the FireBrick® one of your real IP addresses, in which case it should be set the the address of a computer on your network which will normally be switched on. The FireBrick® only borrows this address for specific communications such as time setting requests, and will not normally interfere in any way with the operation of the machine whose address is borrowed. If you do not set this address, or set it incorrectly, then some functions will not work in stealth mode (such as time setting from an external server).

Note: Setting the stealth IP is not the way to give the FireBrick® an IP address. If you want the FireBrick® to be on your network with a normal IP address, use the subnets menu.

Time setting

For logging and for profiles to operate on a time basis properly the FireBrick® must know the time of day and day of week. Being connected to the internet this is done using time servers on the internet.

In order for the time setting to operate the FireBrick® must know a route to the internet (set the default gateway route) and if it has no IP of its own then it must have one defined (stealth WAN IP address). Once this is set the FireBrick® can set the time automatically. The status screen will show if the time is set.

The default time servers are time−a.nist.gov and time−b.nist.gov, two US government time servers.

The time server uses standard internet RFC868 time protocol on UDP port 37. It sets the time once per hour at an arbitrary time during the hour. You can configure a time profile to restrict this to certain times of day and days of week if you prefer (useful if you have an ISDN router and intranet access costs call charges). On power up the time is also set. If the FireBrick® cannot set the time it will keep trying for 2 minutes, and then give up for about an hour before trying again. Once the time is actually set will it stick to the time profile you have selected.

Note that you may find you are logged out as soon as the clock is set for the first time (e.g. just after setting the gateway). This is normal − the FireBrick® thinks you have been logged in for 30 years and times you out!

Syslog IP

syslog is a system logging protocol. To use this you will need a syslog program. This is standard on unix systems (but may require the −r option to allow remote syslog). There are also syslog programs available for Windows.

Once you have a syslog server set up you can set the syslog IP address for that server. This will log various system messages from the FireBrick®. You can set network filters to generate logs when specific traffic is rejected or accepted.

DNS

The FireBrick® acts as a DNS relay. This means that it will accept requests to look up names on the internet, and send these on to a real DNS server. You can set all of your machines on your network to use the FireBrick® as the DNS server, and set the FireBrick® to relay these to a DNS server provided by your ISP. Simply enter the DNS server address you require.

If the FireBrick® is a DHCP server then it gives its own address as the DNS server, and relays requests to the real DNS server.

Log/Filter Options

The log options control when and where log entries are created for various types of event. This also controls what happens if there is no match in the packet matching − this allows you to allow, drop, reject, or bounce unknown connections generally.

The stealth controls allow you to turn off various aspects of stealth operation. These are for advanced use. If you are using the FireBrick® only as a router, you can turn off stealth completely.

The default filter controls the logging of sessions that do not match any other filter, and importantly, this also controls whether the session is allowed or not.

A number of other system events can cause logging :−

Event	General event (e.g. FireBrick power up)
Alert	Unexpected event (e.g. duplicate IP seen on network)
Debug	Additional information, particularly DHCP and unexpected ARP events
Login OK	When someone logs in
Login Bad	When someone fails to log in
DHCP OK	Normal DHCP events, such as allocation of an IP address
DHCP Bad	Problem DHCP events, such as duplicate IP, unable to set an address, etc
Ping scan	Machines going on and off line as a result of profile monitoring
Large sessions	Sessions where more than a specified amount of traffic was transferred

You can also set the server IP address for emailing (where filter/log option *Email* is selected). You can set the from and to address of the email, and some hold off times. The first time is a hold off before sending an email − allowing other emailable log events to be included in the email. The second is a hold off after the email − allowing you to ensure you don't get a flood of emails. You can also restrict emails to certain time periods. Note that once within the time period, any emailable entries in the log are emailed, even if caused outside the time period − but this would all be in one email to catch up with the log. The log has a finite size, and data may be lost from the log if the delay before sending is too long.

UI Options

A number of the User Interface options can be set :−

Pad IP to three digits	If set, all IPs are padded to 3 digits, e.g. 001.002.003.004 instead of 1.2.3.4 Also, ranges are shown in full, e.g. 192.168.001.000−192.168.001.255 instead of 192.168.1.0−255 Note, you cannot normally type such address in to a computer as it may see them as octal.
Number grouping	All numbers over 1000 can be grouped with a comma, dot, or space. e.g. 23,656,232 instead of 23656232 This makes logs showing amounts of data transferred easier to read.
Decimal point	When decimal values are shown, the decimal point can be a point or a comma
Date format	The date can be ISO (2000−02−28), US (2/28/2000), UK (28/2/2000) or full (28th February 2000)
Protocol input	You can select protocols on filters, etc, using a basic pull down menu giving the choices Any/ICMP/UDP/TCP, a pull−down menu giving a full list of protocols, or an input box in which to type the protocol number.

Security

The security option is described in user security.

Advanced Filtering

The main FireBrick® configuration pages provide a list of filters which you can control. This list is just part of the full filtering that can be configured.

Before you can access the filtering controls you must have set the necessary security settings. See user security for details. Note that some of these features are only available on the FireBrick®Plus.

Basic principles

The internet uses three basic protocols (ICMP, UDP, and TCP), two of which have ports (TCP & UDP). These protocols are used for a variety of different applications. There are other protocols as well (over 100 of them), but these are not generally used. Messages on the internet are always sent to and from IP addresses.

If you want to control the filtering on your FireBrick®, you have to understand what you want to filter and why. In some cases you may want to make a specific operation work − a specific application for example. Usually, where there are firewalling issues, the manufacturer will provide details of firewall settings required on their web site. Real Audio is a good example where the full details of the protocols and ports used are on the Real Audio web site − but included as a default filter in the FireBrick®.

When a connection is first made between two computers − which may be from your LAN to the outside (WAN), or from the outside(WAN) to your LAN, a packet of data is sent. This establishes a *session*. For TCP which is used for mail, web, ftp, and many more protocols, this *session* is formally defined and has a start and an end. For UDP and ICMP the session is less formal and uses a timeout to tell when it has finished.

Establishing a session is what is filtered. You can control if a session is allowed to be establish or not based on the properties of that first packet (protocol, port number, IP addresses, etc). Once established, the session continues, allowing the reply packets through automatically. Even if you change the filter later, the session continues.

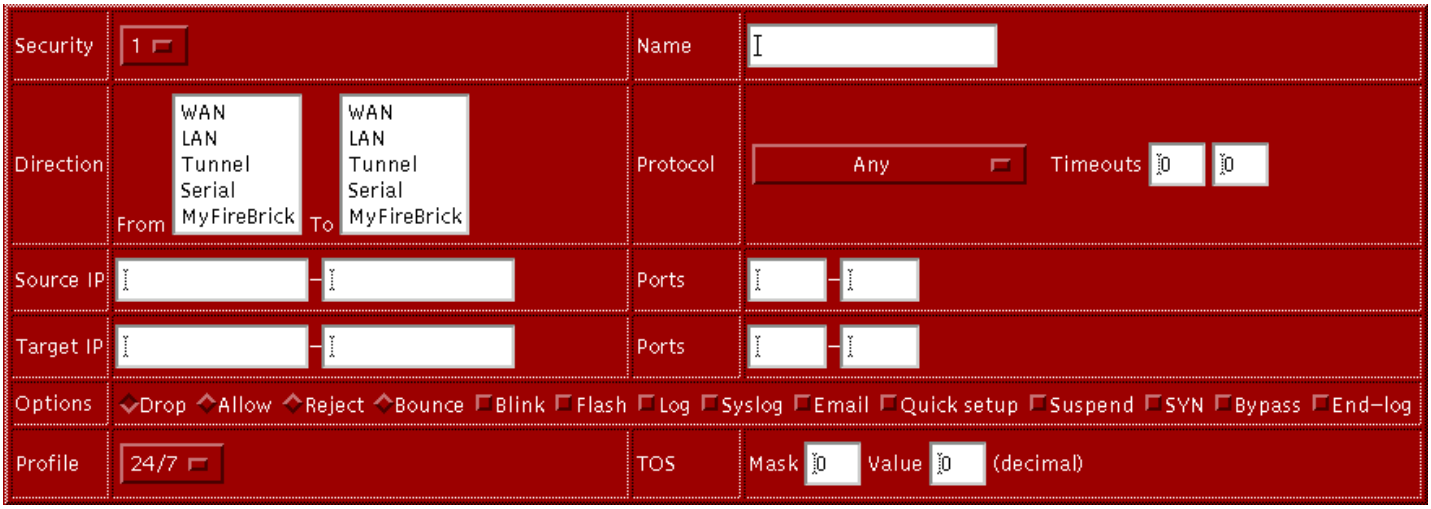
This means you only have to specify the filtering for the establishing of sessions. You do not have to try and set up filters that allow for the replies to established sessions. This makes the FireBrick® more secure than simple filtering without session tracking as only the exact replies are allowed rather than allowing anything that might be a reply. This also makes the FireBrick® easier to configure.

This does however mean you have to consider the direction that the session is set up. For example − web browsing by your users may seem to be data coming in to your network (and indeed they are), but the session is set up by an outgoing request. The action to get a web page is started from inside your network by someone clicking on a link and they make the session − so the direction for web page access from your users is *outgoing− LAN to WAN*.

A number of filters are set up by default. You can delete these filters, change them, or add to them as you wish.

Filter options

The filtering options are as follows :−



Security	The security level controlling access to this filter
Name	The filter name − give a meaningful name
Direction	Select where the packet is going from and to. Multiple selections can be made in each
Protocol	Select the internet protocol which you wish to filter. If you select Any, and have any ports set, then this is UDP or TCP only
Timeouts	These allow the initial timeout, and ongoing timeout to be set. Leave at 0 for defaults.
Source IP	Select the range of source IP addresses that much match − blank for any
Source ports	Select the range of source port number − blank for any. You do not normally need to set this as source port number is rarely relevant.
Target IP	Select the range of target IP addresses that much match − blank for any
Target Ports	Select the range of target port number − blank for any.
Drop	Do not allow the session − ignore the packet
Allow	Allow the session and all replies
Reject	Do not allow the session − send back a packet indicating there is a firewall in place
Bounce	Do not allow the session − send back packets to confuse the originator if possible
Blink	Flash the red ALERT LED once (if lots of packets, then flashes at a steady rate while they are arriving) Only applies when session set up, not for every packet in allowed sessions
Flash	Set the ALERT LED flashing until cleared
Log	Cause an internal log of the session
Syslog	Send a syslog log entry
Email	Cause an emailed log entry
Quick	Include this filter on the main login page as a quick setup item
Suspend	Ignore this filter
SYN	For TCP sessions, only allow the session to be set up if this is a start of a session (SYN, no ACK) This means that existing sessions are not re−established, e.g. after power cycling
Bypass	Allow the traffic but do not set up a session. The replies are not automatically allowed.

	This is mainly used where port scanning, or something generating lots of sessions
End−log	Log the size of the session at the end, as per *Large session* but regardless of length.
Profile	Control when the filter applies. Out of profile filters are ignored
TOS	Restrict traffic to specific types of service (TOS). These fields are decimal mask and value. 0 is default.

Timeouts

Each filter can have two timeout values set. If 0/blank then the defaults are used. These control the initial timeout and the ongoing timeout of a session. The initial timeout applies while packets have only been seen in one direction. The ongoing timeout applies when packets have gone in both directions. These can be fine tuned for specific applications where sessions may need to be dropped quickly or kept open longer.

Ordering

All filters are considered in order from the first to the last, and as soon as as filter (which is within profile and not suspended) is found then it is applied. This means the packet is allowed, dropped, rejected or bounced. No more filters are considered once there is a match.

Always consider the ordering carefully. If a filter does not seem to be having the desired effect the look at all of the earlier filters so see if any of them could be matching. The diagnostic session tracking and log can show which filter was actually used. Feel free to delete unwanted default filters.

If there is no matching filter then the packet is handled according to the default filter rule in the setup menu (normally dropped) unless it is from the FireBrick® itself or to the FireBrick® from the LAN (inside) − e.g. access to web config pages. There is also a default first filter that ensures you are unlikely to lock yourself out. If you want to allow access from the outside for web pages, then you will have to enable the Firebrick−remote default filter as well as setting appropriate user access controls.

Your can move filters around by clicking on the green dot next to a filter and then clicking on where you want the filter to be moved to. This shuffles the intervening filters up or down as necessary.

Direction

The direction is the direction the session is established. Normally this is WAN−>LAN for incoming and LAN−>WAN for outgoing. The direction can include WAN, LAN, Serial, Tunnel, or the FireBrick® itself, and multiple interfaces can be selected. You should be careful of using Any (i.e. all directions selected) unnecessarily as this could cause the config web pages to become inaccessible! (see Don't Panic). Serial is for future use.

Dropping sessions

Rejecting a packet and dropping a packet are not quite the same. Rejecting a packet means that a message is sent back which effectively says "you have been firewalled" (the originator may or may not be able to tell that this is the problem). Dropping the packet simply means it does not get through. Bouncing connections simple causes confusion − but does not allow anything in to your network. Note that rejection and bounces are all delayed so that any attempt to flood you with packets does not block up you outgoing connection with your replies.

Understanding Routing

The FireBrick® is very flexible, so even if you understand routing you should read this section of the manual.

The FireBrick® has to be able to handle stealth routing, normal routing, source routing, IP/port mapping and network address translation. This means the normal simple rules applied to normal routing tables are not quite up to the job.

Basic principles

All computers that use the internet have an *IP address*. This normally written as four numbers with dots, e.g. 192.168.1.25

Computers communicate on the internet by sending messages (packets) from their IP address to another IP address. On this basic principle the whole of the internet is based. Getting a web page involves your computer sending packets from its IP address to the IP address of a web server somewhere else in the world, and that web server sending packets back to your computers.

The trick is how the packets get to the right place. With an address like "25 Arcacia Avenue, NORWICH, UK", it is easy to see that there are different parts that define the location in every closer steps. The 25 is meaningless to the sorting office handling the mail being sent from New York to that address, but the UK bit matters. As it gets closer more bits of the address matter until your postman actually looks for a house with 25 on the door.

With the internet, it is a bit like that, but the addresses are not as obvious for people to understand.

Local area networks

Computers are usually connected together in groups using a local area network. This is normally done with cables. The network will normally have a router connecting it to the rest of the world − such as the router on the end of a leased line or ISDN or ADSL line. The FireBrick® can be a router on your network.

Somehow the computers on the network need to know when to send things to other machines on the same network and when to send them to the router for the outside world. In either case, they also need to know where on the local network to send the information. This is all based on the IP address.

You will have noticed that all of the computers on your local network have similar IP addresses. Usually the same first three numbers, and then even the last numbers may be in a small range. This is no accident, and is part of how local networks are managed.

A network is set up with a *subnet mask*. This is a number (e.g. 255.255.255.0) which is used to restrict the IP addresses. When the mask has 255 in it that means that the number must match, and when it is 0 then any number will do. So if you have 192.168.1.25 as an IP address and a mask of 255.255.255.0, then 192.168.1.59 is on the same network as the first the numbers are the same and the last can be any number. This gets more complicated when the mask is not only 255 and 0. Other numbers constrain the range using binary maths. Fortunately, if you set up an IP and netmask in the FireBrick® subnet settings it will tell you the actual range of IP addresses that is covered by that configuration.

All computers on a network must have different IP addresses, and the same netmask, and must be on the same network (which depends on the netmask). When sending a packet to another IP address on the same network the computer will try and find it directly using an Address Resolution Protocol (ARP). This is a special packet that is sent, and asks "who has IP address 192.168.1.59". The answer specifies which computer it is on the network so that packets can be sent.

To send information to addresses that are not on the network, the computer sends to a *gateway* address. This is set up in the computer as the address on the local network of the router − the gateway to the internet. The computer then uses ARP to find the router and sends the packet to it.

Conventional routing

With a simple computer on a network, routing is simple: If the target is on the same network send directly, and if not send via the gateway.

A router however has a potentially more complicated job. It will have one or more network connections, and may have other types of connections such as a leased line, or ISDN dialup (or in the case of the FireBrick®Plus, tunnels).

This means it is not a simple question of sending everything you don't know to a gateway.

Normally each network interface has an IP address and netmask. This makes part of routing simple − if the packet is for an address on any of these interfaces then send to that interface directly.

Then, there is normally a list of routing rules. These say that if the packet is going to a specific range of addresses (using an IP address and netmask) then send the packet to a specific interface or other router.

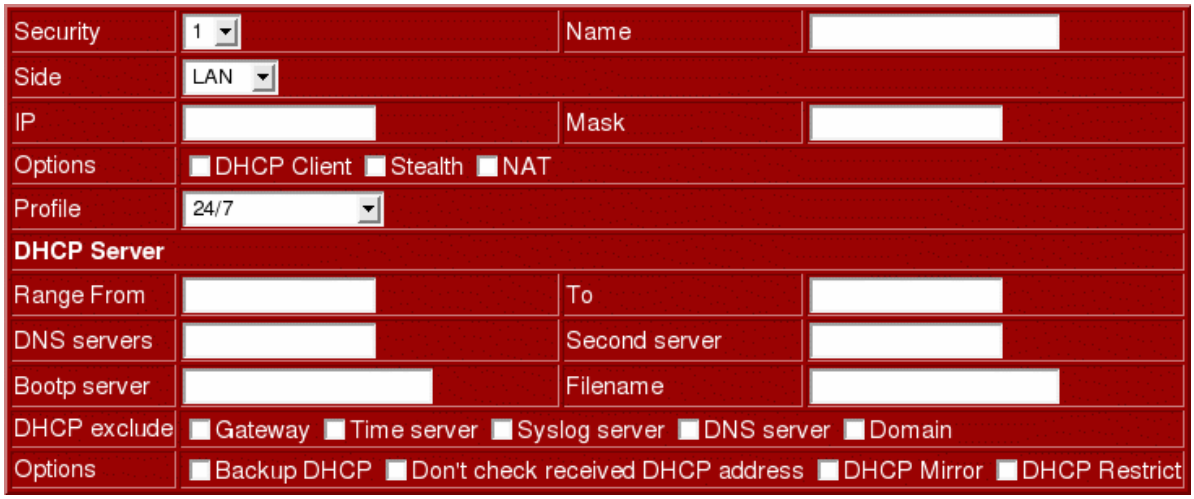
Conventional routing will usually find the most specific match and works only on where the packet is being sent (the destination IP address).

FireBrick® subnets

The FireBrick® allows each interface (LAN/WAN) to have multiple IP addresses and netmasks. This is called *multihoming* and allows you to run several different networks on the same network cabling. This can be for many reasons for this, but simple installations will only have one address and netmask each side.

The FireBrick® subnet control page lets you define the subnets attached to the WAN and LAN connections, specifying an IP address and netmask.

The FireBrick® is also very flexible and actually allows the same IP addresses to exist on LAN and WAN.



Security	Defines the security level controlling who can view/edit this subnet
Name	Give the subnet a name. Generally this is any name you like, but can use used to restrict DHCP
Side	Select if WAN or LAN
IP	Define the IP of the FireBrick®.
Mask	Define the subnet mask. May be entered as a mask (e.g. 255.255.255.0) or bit count (e.g. 24)
DHCP Client	IP, Mask, and other settings are set automatically by DHCP
Stealth	The same addresses exist on the other side of the FireBrick® and so ARPs should be sent through
NAT	This a private subnet, and packets from it must be translated
DHCP Server	Define the range of addresses to allocate as a DHCP server
DNS servers	Define two DNS servers to be allocated by DHCP. If blank, the firebrick acts as a DNS relay.
Bootp server	Define bootp server IP and filename − for advanced use.
DHCP Exclude	Do not accept/issue specific general settings in DHCP mode
Special	Various special DHCP settings described in the DHCP section
Profile	When the subnet is valid

It may seem odd having a profile for subnets, but this can be used to allow multiple redundant routing. i.e. two FireBrick®s can share a single IP, with one dependant on a profile based on being able to ping the other (on a different IP). This allows for one FireBrick® to normally be a "gateway" and the second to be a backup if the first fails.

FireBrick® routing

The FireBrick® routing control tables are an ordered list of routing rules. (conventional routing does not care about the order but finds the most specific rule, the FireBrick® is different and so more flexible).

This means that the order of routing rules is very important. The way routing is done is as follows :−

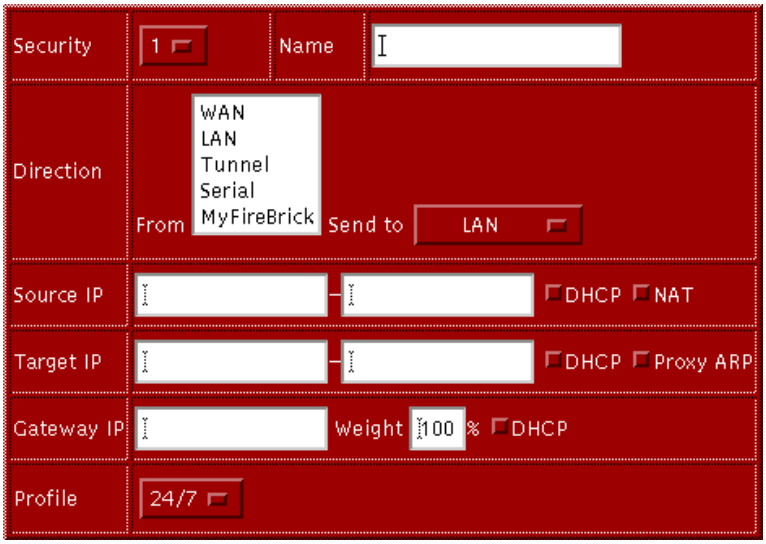
- The routing rules are checked in order and if found then that is used.
- If no match then the target is checked against the subnets configured, and if a match found

then that is used.
- Finally, if no match then the default gateway route is used if defined

Once the destination is known, if a gateway was specified, then it must be on one of the local subnets. If no gateway is specified in a routing entry, then the default gateway is used if it is one the right interface.

As with filters, routes can be moved around by clicking on the green dot and then selecting the destination.

Routing is done on where the packet is from as well as where the packet is to. It is also important to say which connection the packet came from and which it must go to (WAN or LAN, etc). This is important as there could be the same addresses both sides and you may want to route them differently.



Security	Defines who can view and edit this route
Name	Give the route a name
Direction	Specify when the packet is coming from (may be multiple interfaces)
Sent to	Specify where the packet is to be sent to. Can be Any, in which case further routing rules are checked (used to force NAT or proxy ARP)
Source IP	The range of IP source addresses − blank for any
Source DHCP	Indicates that this range is in fact DHCP allocated. A DHCP allocation on any interface in the source direction will cause this range to be changed
NAT	This indicates that any packets following this route are to be translated with NAT
Target IP	The range of IP target addresses − blank for any
Target DHCP	Indicates that this range is in fact DHCP allocated. A DHCP allocation on the sent−to interface will cause this range to be changed
Proxy ARP	Indicates that any request on the direction interfaces for the target range of IPs is to be answered by the FireBrick®.
Gateway	Specify the gateway − relevant where the packets go to another router on the LAN or WAN
Gateway DHCP	Indicates that the gateway is set by DHCP. A DHCP allocation on the sent−to interface will set this

Weight	The weighting for this route, normally 100%. This can be used to allow sessions to follow different routes based on probability.
Profile	When this route is valid

Diverse routing

The weighting on the route can be set at levels below 100% to allow a random chance of a session being routed down that route. If you have several routes you can set multiple routing entries that have different weights, e.g. 50% and 50%, or 33%, 33%, and 34%, or 50%, 30% and 20%. This would normally apply where you have multiple internet connections. It is likely that one of the routes has NAT selected as you will probably have different IP addresses on each internet connection.

Source routing

Unlike conventional routing, a packet can actually be directed based on where it is from as well as where it is to.

Stealth

Normally, with no subnets or routes, the FireBrick® allows messages through it as if it was not there (apart from filtering rules). This means that it allows the ARP requests to *find* a machine through it, and the replies back. The log/filter options allow stealth to be disabled.

If you configure a subnet on an interface, then this means that the FireBrick® has a real IP address, and that all of the addresses on that subnet are on that side of the FireBrick®. If the FireBrick® receives an ARP from that side for another address on that side then the FireBrick® ignores it (not sending to the other side). Also, broadcast packets (being sent to the first or last address on a subnet) are treated as being for the FireBrick® itself − so it will answer broadcast pings and DHCP requests. The log/filter options allow broadcasts to be stopped.

If you want the FireBrick® to have the same subnet each side and to pass ARP requests and data using stealth, but still want it to have an IP address, then you can mark the subnet as *stealth*. This means that the FireBrick® considers itself to have the IP address you have said, but that it still sends ARP requests and broadcast messages to the other side as it did not have a subnet of its own. This is useful if you have a FireBrick® in the middle of a network without the rest of the network knowing, but still want to give the FireBrick® an IP address.

If the FireBrick® sees ARP requests for addresses that are not on any subnet then is passed them through (but the log/filter options allow this to be disabled).

It is important to realize that stealth packets do not go through the routing table. If you need them to you must set a proxy ARP route.

Proxy ARP

Sometimes there is another router which is handling traffic for a part of an existing subnet. All computers on the subnet assume that these addresses are on the local network and don't go looking for a router.

The FireBrick® can be configured to automatically direct such packets to the router by responding for them when an ARP request is sent. This is the *Proxy ARP* setting in the routing table. It causes the range of target addresses specified to be answered by the FireBrick® on the source interface.

When packets are received for those addresses they are routed according to the routing rule − which may be to send to a specific interface or to send to another router.

Normal routing

If the FireBrick® is set as a gateway address for any machine or is proxy ARPing for some addresses, it will receive traffic for IP addresses that are not its own. When this happens it puts the packets through the routing table as described above.

Once the packet is routed and a session is established, that route remains in place for the session (important is routes change on the fly, such as switching to/from ISDN backup, etc).

Multiple gateway load sharing

The FireBrick Plus allows for multi−gateway load sharing. To use this you will need multiple external gateways such as multiple ADSL lines. If these are on different subnets then you should set each as a subnet on the FireBrick. Pick a gateway address on the subnet for the external link on which you want the replies to arrive (e.g. if you had a 2Mb and 500K ADSL you would want to use an address on the subnet for the 2Mb line). This should be an unused address, and can be the subnet network address as it is simply used to tell teh firebrick to use the multi−gateway list. Then complete up to 4 gateways.

When any traffic is directed to the gateway that is the default gateway, it will have its gateway changes at the last moment, on a per packet basis, to one of the 4 gateways you have listed in a simple cycle. This allows you to bond multiple uplinks on ADSL lines for example.

NAT

Sometimes it is necessary to configure a set of private addresses which have a single point of access to the internet.

Private addresses have been reserved for this purpose and are 10.X.X.X, 172.16−31.X.X and 192.168.X.X. You should not use any other addresses for private networks.

The FireBrick® can be configured with subnets each side − e.g. a private network on the LAN and the public network on the WAN. This means packets can be routed from one side to the other with no problem.

The issue is that the private addresses will not work in the internet − they are not real addresses, and replies could not get back.

In this case, simply mark the LAN subnet as NAT. This means that all messages from your computers on their private addresses have the source address changed to that of the FireBrick® as they are sent out. Replies coming back have the destination changed back to the private address. This only applies where a specific routing rule is not found, so if you add special routing rules, and still need NAT then you have to set the NAT checkbox in the routing entry. It also means you can have rules which stop NAT happening to/from certain addresses by adding a routing rule.

Some protocols and some games can't cope with this type of operation and require real addresses − in particular ftp will need passive mode set or cleared to operate correctly.

Note, that whilst NAT will map IP addresses for protocols other than ICMP, TCP, and UDP, there is no way to track multiple sessions as the FireBrick cannot allocate a port or ID. As such NAT for

such protocols can only be relied on where there is only one session at a time. If multiple sessions, then replies may go to the wrong one depending on the last session that was active.

Portmapping

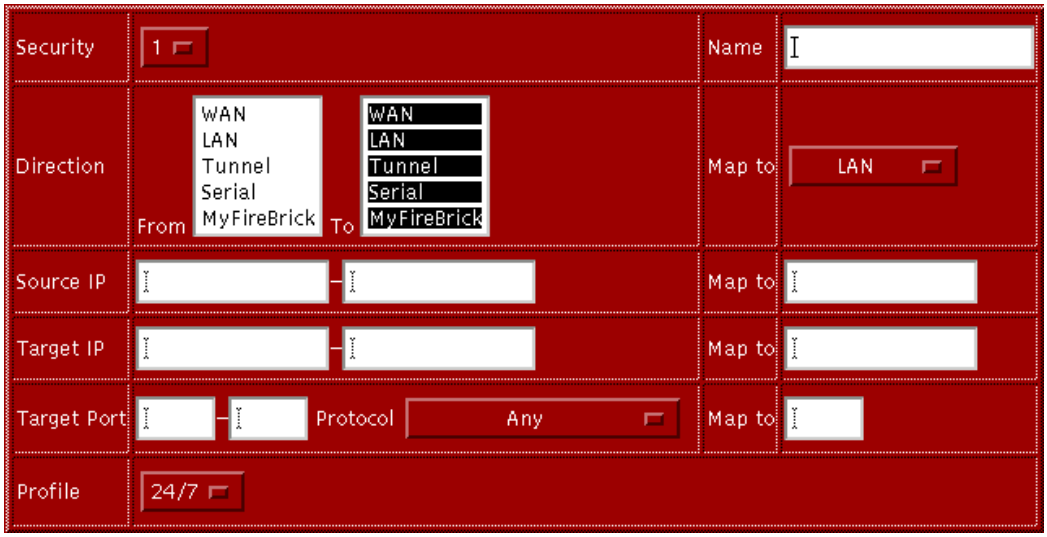
When you have a set of private addresses within your network (e.g. using NAT), then you may still want to be able to run servers such as SMTP mail. This means allowing new connections in to your private network.

This cannot work with private addresses, so a facility called *portmapping* is provided to allow IP/ports on the FireBrick® to be mapped to ports on specific machines on your network.

Port mapping is quite general purpose, and can also allow outgoing translations (accessing one IP actually accesses another), so could be used to force use of web proxies, etc.

Like most such tables the first match is applied. If out of time profile the entry is skipped and a later match is found.

Port mapping rules apply to all sessions, even stealth sessions, and if matched force the session to be routed. As such, port mapping rules can be used to hi−jack stealth traffic. By setting a target of Any in the port map, you can hi−jack traffic and force it to follow the normal routing rules, without necessarily changing the IPs or ports !



Security	Defines who can edit or view this portmap
Name	Name the portmap
Direction	Allows the existing routed/stealth direction of the packet to be checked. This can be multiple selections
Map to	Says where the packet is to go instead − Any means that the packet is routed
Source IP	The range of source IPs to check − blank for Any
Map to	The new source IP − blank for no change, 255.255.255.255 means set to the FireBrick® itself
Target IP	The range of target IPs to check − blank for Any
Map to	The new target IP − blank for no change
Protocol	The protocol to check
Target port	The range of target ports to check − blank for any

Map to	The new target port − blank for no change
Profile	When the port map applies

Setting an IP address

Stealth − no IP

The FireBrick® can be accessed using a stealth IP address (my.FireBrick.co.uk) from the LAN side if it is part of an existing network. This works right out of the box.

However you may also want to be able to set the time which requires an IP address that will get back to the FireBrick®. All you have to do to ensure that the time works is to set up a WAN stealth IP address which is one of the addresses of a computer that is normally on your LAN and turned on, and also set a gateway route address. Both of these are in the set up screen.

This will allow time, and if you wish syslog and email, to be sent externally apparently from a machine on your network. The FireBrick® will pick up the reply to the requests it sends but will not otherwise interfere with the normal working of the machine you have picked. The machine needs to be switched on to allow your internet router to send the packets which the FireBrick intercepts.

Stealth − with IP

Even if basically operating in a Stealth mode you may want to provide a real IP address to your FireBrick®.

Assuming you have a subnet of public IP addresses already, and have a spare IP address for the FireBrick®, then you can set up an IP address as follows :−

In this example we will assume that you have IP addresses 123.4.5.0/28 i.e. you have the range 123.4.5.0 to 123.4.5.15. Your router is 123.4.5.1 and you have picked 123.4.5.2 as the address for the FireBrick®.

1. Set the LAN subnet to the FireBrick® IP (e.g. 123.4.5.2) and the subnet (e.g. 255.255.255.240) and set stealth mode
2. Set the WAN subnet the same
3. Set the default gateway route to 123.4.5.1 on the WAN

In this case the computers on your network will use the outside router as their gateway address, and the FireBrick® will respond from either side as 123.4.5.2.

Routed

You can give your FireBrick® a genuine IP and subnet each side if you wish. Some networks (e.g. radio internet connections and cable modems) will give you an external IP and gateway address as well as an internal IP and netmask.

For example − your ISP has allocated you an external address of 123.10.20.56/24 and a gateway of 123.10.20.1. You also have a block of addresses 123.4.5.0/28 allocated and you will make the FireBrick® 123.4.5.1.

1. Set the WAN subnet to the outside addresses (e.g. IP 123.10.20.56 mask 255.255.255.0)
2. Set the LAN subnet to the inside addresses (e.g. IP 123.4.5.1 mask 255.255.255.240)
3. Set the default gateway route to 123.10.20.1 on the WAN

In this case the computers on your network will use the FireBrick® LAN IP address as their gateway.

Private with NAT

You could have the situation where you have a block of addresses allocated, but no inside addresses. This the same as above except that the inside addresses are a private range you pick (e.g. 10.0.0.0−255) and you should set the NAT tick box on the subnet.

DHCP with NAT − e.g. cable modem

Simply set a subnet for LAN with a private address and range and NAT set, and set a WAN subnet with DHCP client set (no other values needed). The cable modem will allocate the FireBrick® the network address and subnet as well as a gateway. Machines on your local network use the firebrick as a gateway and DNS servers.

You could set a range of IP addresses on your LAN subnet for DHCP serving to machines on your LAN.

Automatic IP allocation

DHCP (Dynamic Host Configuration Protocol) is a system that allows IP addresses to be allocated on an network automatically.

The FireBrick® can issue addresses on a network as a DHCP Server, and can receive its IP address automatically as a DHCP client.

DHCP server

The FireBrick® will allocate up to 256 addresses on LAN or WAN, and the diagnostics page will show the addresses that have been allocated along with the machine name if known. Whilst each DHCP lease is only 2 hours long, the FireBrick® will keep track of old leases to ensure machines always get the same address even if it has been a long time since they were last on your network. This allows a semi−permanent allocation of IP addresses. Only if addresses run out will old ones be re−used.

To be a DHCP server simply requires that the subnet configuration has a range of IP addresses to allocate (and is not stealth). The addresses allocated are in the range specified where they are also valid on the subnet you have configured and obviously avoiding the FireBrick®s own address.

You can set up several identical subnets with different ranges of addresses to allocate for DHCP if required − this will allow several different ranges to be given out − perhaps avoiding addresses used for other purposes. If the requesting machine has a name that matches a restricted subnet, then it will only be allocated an IP from one of the restricted subnets for which it's name matches. If the requesting machine does not match a restricted subnet, then it can only be allocated from unrestricted subnets.

The FireBrick® automatically avoids giving addresses where there appears to be another machine already using the address, but careful planning should avoid this anyway.

You can also set *Backup DHCP* which means that the server will not answer the first request from a machine − allowing another DHCP the chance to answer first.

Normally the DHCP server provides DNS, Gateway, Domain, time server, and syslog server − however these can individually be excluded if required in the subnet configuration.

Note that if the time is not set, the the server will not track the lease times, but still allocates two hour leases.

DHCP client

Being a DHCP client means that the IP address, subnet mask, gateway address and various other settings for a computer are set automatically. On the FireBrick® this allows the IP, subnet mask, gateway, DNS server, Time server, Syslog server, and Domain to be set. Some of these can however be excluded allowing them to be set manually.

To be a DHCP client you should configure a subnet with and mark it as DHCP client. Going back to the subnet later, or looking at DNS server, etc, will show the current values. The diagnostic page also shows the DHCP server details.

Options

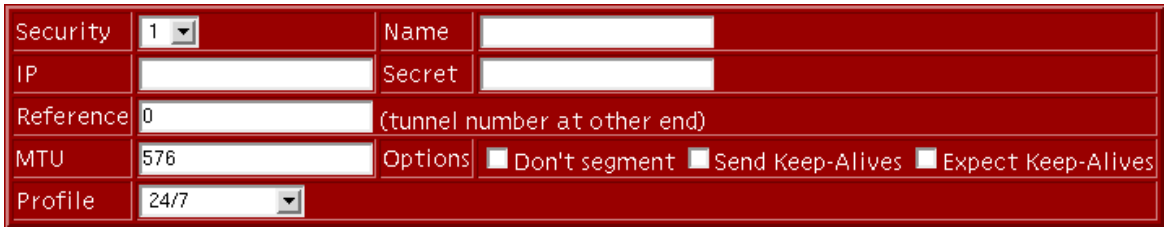
Backup DHCP	As a DHCP server, the FireBrick® does not answer the first query from a host, allowing another DHCP server to answer first.
Don't check	As a DHCP client, the FireBrick® does not check the address it is given is valid − needed on some cable modems
DHCP Mirror	As a DHCP server, this subnet is configured based on the other interface as a DHCP client. This makes the FireBrick® have the far side router address, and allocating a DHCP address if was given on the far side
DHCP Restrict	As a DHCP server, this subnet is only used when the client machine name starts with the subnet name
Broadcast renewal	As a DHCP client, when renewing addresses the request is broadcast rather than sent to the previous server

Virtual Private Networks

The FireBrick® allows network tunnels to be created. This allows a virtual private network to be created.

Tunnels can currently only be created between FireBrick®s. The tunnel carries an encryption code so that it cannot be tampered with or forged, but it not encrypted for secrecy. The tunnel uses UDP which should survive going through other routers and translation, but one end must be on a fixed IP.

The tunnel set up is as follows :−



Security	Who can edit/view this tunnel
Name	Name the tunnel
IP	Set the IP address of the far end − blank for any allowed
Secret	A secret − blank for no secret
Reference	Set the tunnel number at the far end
Profile	When the tunnel applies
MTU	You can safely leave this at it's default − it controls the maximum packet size used
Don't segment	This forces the packets sent to fit in the maximum segment − use for special applications
Send Keep−Alives	This makes the tunnel send a small message every second to ensure the tunnel stays running. Useful when tunnelling through another router which is performing address translation
Expect Keep−Alives	This causes a log event when the tunnel starts and stops working − i.e. it expects the regular messages from the other end. If they stop then the tunnel will forget any dynamic IP address that the other end may have been using.

At each end you must create a tunnel. The reference at each end must be the tunnel number at the other, and the secret must be the same at both ends.

One end, and ideally both ends, must have the IP address of the other. It is possible for one end to have no IP address − in this case it cannot start communications on the tunnel. Once it has received some information on the tunnel and confirmed it is valid then it will note the IP address it came from and use that for all replies. This allows for one end being on a dynamic address.

The routing rules then have a To address which is of the form Tunnel(name) allowing you to specify what traffic goes down a tunnel. Ensure you create routing rules for addresses at the far end of the tunnel (at each end).

Remember that stealth packets do not go through the routing rules, and also that proxy ARP will

only be useful if the addresses are on the network at the source end. i.e. the FireBrick® should be configured as a gateway for tunnel routes to work or should be routing a part of the addresses on a LAN using proxy ARP.

Notes:

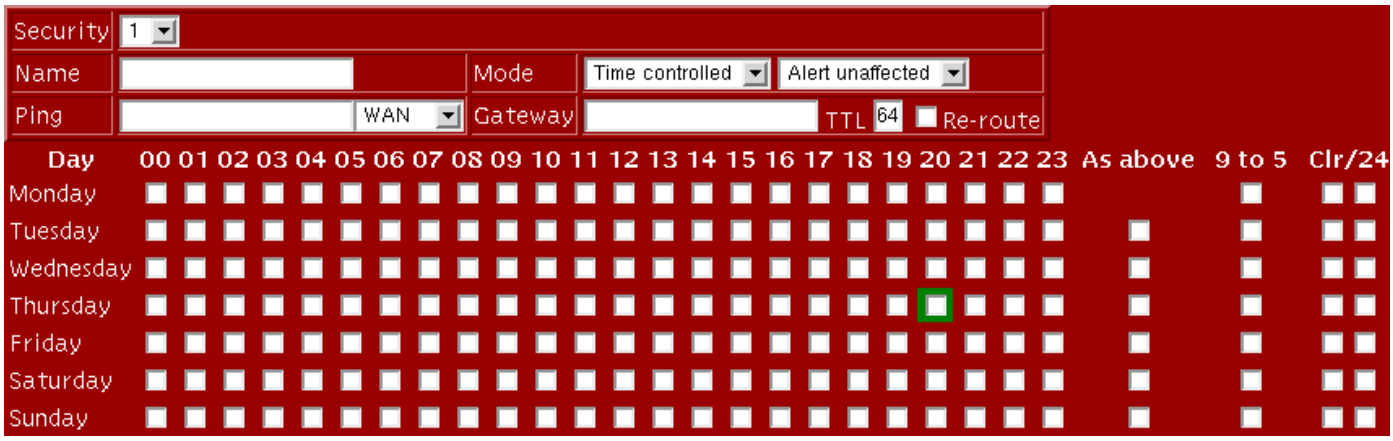
Tunnels are normally signed but not hidden. This means your traffic may be visible to others if someone can snoop the network between the tunnels, but they cannot forge communications or change the contents. If you leave the secret blank at both ends then the tunnel is unsigned. This means it is simply a way of mapping IP addresses and privides no security other than checking the IP address the packets came from. In some situations this is quite adequate security.

Profiles

Most of the configuration settings in the FireBrick® have a *Profile* option − restricting when they apply.

Profiles can be used as a simple time of day and day of week control, or can be used as a master switch allowing complete sets of routes and filters to be turned on or off manually. They can also be used to monitor a specific IP address via a specific interface − this allows automatic fall back plans to be controlled based on a failed link (e.g. ADSL falling back to ISDN).

A number of time profiles can be created :−



Security	Who can view/edit this profile
Name	Name the profile
Normal timed	The profile is active during the hours indicated
Permanent enabled	The profile is always active
Permanent disabled	The profile is never active
Ping scanning	The profile is active while a host is responding
Alert affected	The alert LED can be set to come on if the profile is active or not
Ping	Define the address interface on which to send the ping. *Any* means routing rules are followed
Gateway	Define the gateway/router via which the ping is sent. Blank means routing rules are followed
TTL	The time to live for the ping − how many hops it will go before giving up. Can be useful to ensure the ping is being monitored via a specific route.
Re−route	This causes traffic in progress to be re−routed if this profile changes
Time grid	Defines what hours the profile is active (or when to ping) Various shortcuts apply when saving, edit again to see what they have done.
As above	Shortcut − used to copy the whole of the previous day
9 to 5	Shortcut − sets hours from 9am to 4pm (i.e. time 9−5)
Clr	Shortcut − clears the day
24	Shortcut − sets all hours in the day

Note that the current time is highlighted. If the time is not set the entire time grid grid is not shown.

Profiles can be for various different purposes, and can obviously overlap. Each setting is attached to just one profile. There are 4 pre−defined profiles in addition to the ones that can be set manually − these include 24/7 (always on), 9−5 M−F (9am to 5pm Monday−Friday), 2am Sun (2am to 3am on Sunday), and OFF (never active).

The time must be set which requires a time server and basic routing to be configured. Once this is done profiles can be used based on time and day. If not set then profiles can still be used but only as a master switch or ping scanning. After power on until the time is set the profiles time setting is frozen at the state when the power went off.

Each of the settings that can use a profile show the profile in green for currently active and red for inactive.

Ping scanning

If you select a ping mode, then during the times specified the address is pinged every 10 seconds. This means you will need to set the times (possible using the *24* box to set 24 hours every day).

If there is no response to a ping, then a further 7 pings are done at about 1 second intervals. Only on all 8 failing to respond is the ping considreded a failure. Once failed the ping is once every 20 seconds until there is a reply.

As the ping mode may be used to control routing (e.g. ISDN backup to ADSL), it is necessary for the pinging to continue after the failure (again at 10 second intervals) but to do so via the broken route (e.g. still down the ADSL line). For this to work you can select the interface and gateway for the pings − which bypass normal routing rules.

Obviously many difference aspects of the FireBrick® could be controlled using such a profile (e.g. routing, speed limiting, filters) as these may need to be different when using a slow backup link such as ISDN.

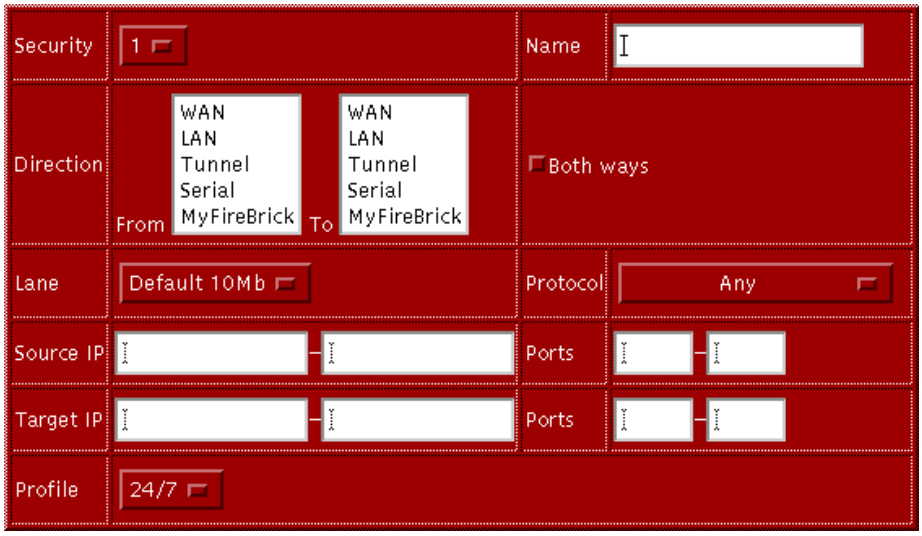
ALERT LED

You can configure the ALERT LED to be lit for a profile being active / inactive. This is useful when setting ping scanning, and can mean the ALERT LED indicates ISDN fallback, for example.

Speed controls

Separately from the filtering and routing, each new session is checked against a speed control list.

This allows the session to be assigned to a speed lane. A speed lane is a single pipe which has limited throughput. The lane can be set to any number of Kb/s (kilo bytes per seconds) for traffic to the WAN or LAN. Traffic is placed in a speed line by a set of rules, the first match applying.



Security	Who can view/edit this entry
Name	Name this shaping rule
Direction	What direction the traffic is going in. Can be multiple selection.
Both ways	Indicates that the rule applies both ways (see below)
Lane	Which speed lane the traffic goes in to
Protocol	Specific protocols that apply
Source IP	The range of source IPs − blank for any
Source port	The range of source ports − blank for any This does not normally need setting as the source port is not normally relevant
Target IP	The range of target IPs − blank for any
Target port	The range of target ports − blank for any
Profile	When the rule applies

The format is very similar to the filtering tables except that a speed lane is selected and there is an option to set "both ways".

Speed is limited using packet scheduling which provides a smooth throughput at the requires speed. Setting a speed lane does not guarantee a minimum speed, it limits to a maximum.

Selecting "Both ways" creates two lane controls − one of which is as shown, and one is the reversal of the Direction and Source/Target IP addresses. Note that the ports are not reversed.

The direction (from/to) relates to the way the session is created − i.e. the first packet.

Unlike filters, you can change the speed and change the rules for controlling the speed lanes at any time and this will have an immediate effect on existing sessions. You can make speed rules dependant on a profile so that changes happen automatically at certain times.

Each speed lane has limits on bandwidth to the Lan and to the WAN. You can also set a lane/direction to give away unused bandwidth, and also to take unused bandwidth from those lanes that give it away. There is also a FastACK feature for advanced users (see the technical rteference manual for more details).

The first speed lane is a master speed lane, which is applied after any other speed lane selected. This allows you to limit the overall speed of all traffic.

Reporting and Statistics

The FireBrick® provides a number of reports and diagnostics.

Statistics

The speed lanes and filters will shows basic usage statistics providing the clock is set. They both show the usage yesterday and so far today as Mb (mega bytes), as well as Last Month and This month. In addition, they show the current KB/s.

Speed lanes	The usage is shown for traffic to the LAN and to the WAN separately
Filters	This shows total traffic using this filter. Bear in mind that this is traffic both ways as a result of this filter, so a filter for all outgoing traffic will in fact show the total of all outgoing traffic and the responses (e.g. the content of web pages that were received as a result of an outgoing request). Look at the speed lane statistics for an indication of traffic in to and out of your network as a whole.

Diagnostics

The diagnostics menu allows you to view information about your network as seen by the FireBrick®.

Serial Number	Your serial number
Time now	The current time (only shown if the time is set)
Clock last set	The time the clock was last set
LAN/WAN	The number of machines *seen* on the LAN/WAN. This is a count from the MAC cache
LAN Usage	The bar graph of current LAN usage
DHCP Server	If a DHCP client, stats the DHCP server address(es).
Link	A green square for each network link on WAN and LAN hub ports
Partition	Indicates of the network connection has been disabled − this happens automatically if there is a fault with the connection
Reversal	Indicates if any network connection has reversed polarity − i.e. the cable is incorrect (does not necessarily stop operation)
Noise	Indicates if there is excessive noise on the link − indicating faulty cable or equipment connected
Sessions	Lists the session stats (how many sessions on each protocol), and allows report of individual sessions with kill option. Note, kill option only if user has edit rights for diagnositics. Can only view sessions associated with filters the user can view.
DHCP	Lists all of the DHCP lease allocations with expiry dates and machine names where know
ARP	Lists all ARP entries − the MAC/IP table used by the FireBrick®. This gives an indication of currently active machines attached to the FireBrick®.
MAC	Lists all machines the FireBrick® has ever seen since last reset.
Sessions	Lists actual sessions in progress.

Log	Shows the current activity log, and stays following the log in real time. Use your browser STOP button if you do not want to continue to watch the log. This may not work via some types of web proxy that cannot cope with *open ended* pages like this.
Counters	Details of stats for the low level ethernet drivers, including current traffic in and out.

DON'T PANIC

Screen says "User Interface Required"

This normally means you have uploaded new software without uploading the language specific user interface file. Go to http://software.FireBrick.co.uk/ and download the language file and upload into your FireBrick®. If you normally have to log in to upload files, you will have to do so before you can upload new files. If you don't have a valid log in − see below on how to factory reset your FireBrick®.

Note − at this screen you can load a new software version (F) file, or a saved configuration file if you require. If you cannot locate the appropriate user interface file, then load the latest software release and then its user interface file.

Configured yourself in to a hole!

It is quite possible to configure a FireBrick® so that you can no longer access it to change the configuration. You must be careful to avoid doing this. It is also possible to simply forget the password you have set − which has much the same effect.

Note that the first filter is a filter allowing access to the FireBrick® TCP port 80 − this is to allow access from the LAN to the FireBrick® administration web pages. Removing this in itself does not stop access unless you have a filter later that blocks this access to the FireBrick®. As such it is a good idea to leave this filter in place until you are sure what you are doing.

To get round this it is possible to *factory reset* a FireBrick®. This does however mean entering all of your configuration again. It is therefore recommended that you regularly save your current configuration so you can restore it after a factory reset. This is also a good security measure as you can restore a configuration if you think someone has been tampering with the settings.

Factory reset

To factory reset your FireBrick®, follow these steps :−

1. Remover power and all network connections
2. Connect a straight network lead (such as the one provided with the FireBrick®) from the WAN (left) to the right hand LAN port.
3. Power on the FireBrick®
4. Observe that the link light on the LAN port is lit and on the WAN port blinks rapidly.
5. After a moment the red ALERT comes on.
6. Remove the network cable with the power still connected
7. The FireBrick® will reset (green and red LEDs go off for a moment), and then start as normal with cycling lights on the hub.
8. The factory reset is now complete − bear in mind that the FireBrick is now operating on the stealth IP as detailed in getting started.

Note: For software issues 1.2.257 and before there is an alternative procedure :−

You need a serial connector. Your dealer can send a suitable cable if you wish or you can make one.

The procedure for factory reset is as follows :−

1. Power off and remove all cables
2. Ensure RI is connected to DTR on the serial cable (pins 9 and 4)
3. Power on, red light is lit for one second and then goes out
4. Power off
5. Remove serial cable
6. Reconnect LAN cables
7. Power on
8. Following getting started instructions to set up configuration.

Whilst we really would not recommend this, it is probably possible to short pins 9 and 4 with a bit of wire, if you are desperate. The loop must be on for 1 second after power on until the red light goes out. Any damage to the 9 way connector as a result of this is not covered by the warranty.

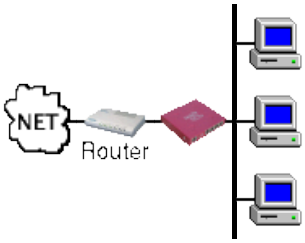
Dead FireBrick

It is quite difficult to get a dead FireBrick®. One way is to power cycle during software upgrade. This results in a FireBrick® which does not work. It may also blink red or green lights repeatedly and the hub lights are likely to come on and fade away after a few seconds. Note that the hub will continue to work as a hub even if the FireBrick® is otherwise non functional as long as it is powered.

If this is the case you can return the FireBrick® to your dealer for repair (for which the dealer is likely to charge). Some dealers may offer a swap out unit as this could take a couple of days.

Examples

ADSL/Stealth



ADSL non−NAT installation
Router has single subnet
PCs using real internet addresses
FireBrick not to use up an address

In this configuration the FireBrick operates in a full stealth mode, not using one of the addresses allocated by the ISP.

1. The FireBrick will operate out of the box with no extra configuration if required
2. PCs on the LAN must have the router address as their gateway address
3. Access the FireBrick config from a PC on the LAN using http://my.firebrick.co.uk/
4. Adjust filters as required

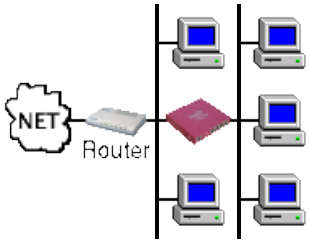
For clock setting, and any external communication from the FireBrick such as emailed logs :−

1. Pick one of the PC addresses for a PC that is normally on
2. Set this as the WAN stealth address in the setup menu
3. Set the router address as the gateway in the setup menu

This example equally applies to :−

1. Any installation with a router and a single subnet
2. BT net start lines
3. Existing network installations with a router

ADSL/Stealth with external machines



ADSL non−NAT installation
Router has single subnet
PCs using real internet addresses
FireBrick not to use up an address
Some machines outside of firewall

In this configuration the FireBrick operates in a full stealth mode, not using one of the addresses allocated by the ISP. Some of the PCs are on the LAN side and some are on the WAN side. This is usually done where the external machines are carefully configured to be secure, but if the external machines are compromised then this does not allow access to the internal machines.

The FireBrick provides no protection for the PCs on the outside.

1. The FireBrick will operate out of the box with no extra configuration if required
2. PCs on the LAN must have the router address as their gateway address
3. Access the FireBrick config from a PC on the LAN using http://my.firebrick.co.uk/
4. Adjust filters as required

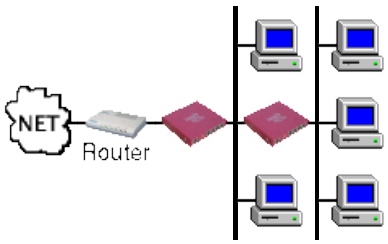
For clock setting, and any external communication from the FireBrick such as emailed logs :−

1. Pick one of the PC addresses for a PC that is normally on and on the LAN side
2. Set this as the WAN stealth address in the setup menu
3. Set the router address as the gateway in the setup menu

This example equally applies to :−

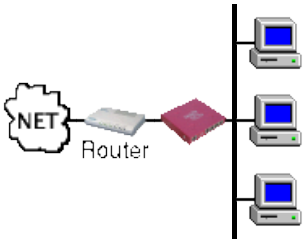
1. Any installation with a router and a single subnet
2. BT net start lines
3. Existing network installations with a router

In such cases, a second FireBrick is normally recommended. In this case, you may wish to change the LAN stealth address of the outer FireBrick to a different address, such as 217.169.0.2, so that it can be accessed from PCs on the inside without picking up the internal FireBrick by mistake.



ADSL non−NAT installation
Router has single subnet
PCs using real internet addresses
FireBrick not to use up an address
Some machines outside of firewall
Second FireBrick provides outside protection

ADSL/Stealth + FB address



ADSL non−NAT installation
Router has single subnet
PCs using real internet addresses
FireBrick allocated a real address also

In this configuration the FireBrick operates in stealth mode but has a real address. This is normally done to allow external access to the FireBrick configuration.

1. Pick an address for the FireBrick
2. Create a LAN subnet with that address and the appropriate subnet, marked stealth
3. Create a WAN subnet with that address and the appropriate suvnet, marked stealth. Ensure this is after the LAN subnet
4. Set the gateway on the FireBrick to the router on the WAN
5. PCs can have the router or the FireBrick as their gateway
6. Always ensure all PCs, and the firebrick subnets have the subnet mask allocated by the ISP.
7. Adjust filters as required

For external access to FireBrick web management pages :−

1. Enable a filter allowing WAN to FireBrick for at least TCP port 80
2. Ensure the admin user has a password, and disable the view and edit rigths for the nobody user
3. Set the required user to WAN access, and the nobody user to WAN access (to allow the login)

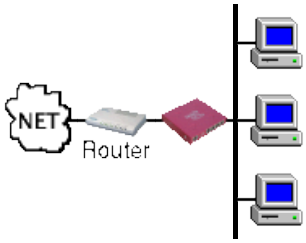
If DHCP allocation to PCs is required :−

1. Set the DNS server address in the FireBrick so the FireBrick can be used as a DNS relay
2. Pick a range of addresses for DHCP use, and set these on the FireBrick LAN subnet
3. Mark the LAN subnet as not stealth − this allows the DHCP server to work correctly
4. Add a route from LAN to WAN with target IP of the router and proxy ARP. This allows access to the router.
5. Ensure PCs are set to automatic IP and (for windows) DNS disabled.

This example equally applies to :−

1. Any installation with a router and a single subnet
2. BT net start lines
3. Existing network installations with a router

ADSL and private network behind FireBrick



ADSL non−NAT installation
Internal machines on private addresses
Port mapped incoming SMTP email

In this configuration there is a routed non−NAT internet feed (e.g. ADSL). The PCs are to be on private addresses. In this example we will assume that the ADSL router has address 123.4.5.1 and the subnet is a block of 16 (/28 or 255.255.255.240).

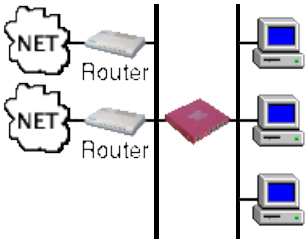
The FireBrick provides a NAT configuration to private addresses :−

1. Allocate a private network address for the internal machines, e.g. 10.0.0.0/24
2. Allocate the FireBrick a private address, e.g. 10.0.0.1 creating a LAN subnet for the FireBrick on this address and subnet 24 (255.255.255.0), set NAT
3. Optionally, include DHCP allocation range on the private addresses to allocate addresses to machines on the LAN
4. Allocate the FireBrick one of the public addresses, e.g. 123.4.5.2 and create the WAN subnet with this address, subnet 28 (255.255.255.240)
5. Set the gateway on the FireBrick to the router on the WAN (i.e. 123.4.5.1)
6. PCs are set with the FireBrick as their gateway (i.e. 10.0.0.1) and subnet 24 (255.255.255.0)
7. You may want to set the FireBrick with an ISP allocated DNS server address, and set the PCs to use the FireBrick for DNS (needed for DHCP use)
8. Adjust filters as required

This example equally applies to :−

1. Any installation with a router and a single subnet
2. e.g. BT net start lines

ADSL with ISDN fallback



ADSL non−NAT installation
ISDN dialup router, NAT
Internal machines on private addresses
Port mapped incoming SMTP email

In this configuration there is a routed non−NAT internet feed (e.g. ADSL) and also a backup ISDN dialup router. The dialup router is using a conventional dialup which provides NAT from a single internet address. In this example we will assume that the ADSL router has address 123.4.5.1 and the subnet is a block of 16 (/28 or 255.255.255.240).

The FireBrick provides a conventional NAT configuration :−

1. Allocate a private network address for the internal machines, e.g. 10.0.0.0/24
2. Allocate the FireBrick a private address, e.g. 10.0.0.1 creating a LAN subnet for the FireBrick on this address and subnet 24 (255.255.255.0), set NAT
3. Optionally, include DHCP allocation range on the private addresses to allocate addresses to machines on the LAN
4. Allocate the FireBrick one of the public addresses, e.g. 123.4.5.2 and create the WAN subnet with this address, subnet 28 (255.255.255.240)
5. Set the gateway on the FireBrick to the router on the WAN (i.e. 123.4.5.1)
6. PCs are set with the FireBrick as their gateway (i.e. 10.0.0.1) and subnet 24 (255.255.255.0)
7. You may want to set the FireBrick with an ISP allocated DNS server address, and set the PCs to use the FireBrick for DNS
8. Adjust filters as required

The ISDN router needs to be configured to allow access whenever it is used :−

1. Allocate a public address for the ISDN router, e.g. 123.4.5.3, and set with subnet 28 (255.255.255.240)
2. Set the default incoming address translation/NAT−mapping to the FireBrick 123.4.5.2 allowing incoming mail, etc.
3. Set up dial on demand internet connection with NAT

The FireBrick needs to monitor the ADSL link :−

1. Find the next hop address on the ADSL (see below)
2. Create a profile called ADSL, set for ping scanning on interface WAN with gateway 123.4.5.1 to the next hop address, set *Alert if inactive*
3. Ensure the profile is set for all day every day (click the right hand box for each day, marked "24")
4. Confirm by reloading the profile index page, after 1 minute, that the profile is active

The normal FireBrick routing will need to be replaced with explicit routing rules allowing for a change to ISDN when required :−

1. Move the *Subnets* route up, and add a new route below it to the ISDN router, target Any (blank), from Any, to LAN, gateway 123.4.5.3 (the ISDN router), select NAT, Profile No−ADSL

If you need specific port maps for incoming mail :−

1. Create a port map, from WAN, to FireBrick, addresses Any, port 25 (may left blank), map target to your mail server, e.g. 10.0.0.2

Incoming email :−

1. Incoming email for SMTP could be set with MX records to go to your FireBrick, e.g. 123.4.5.2
2. The FireBrick would need to allow WAN−>Any port 25 TCP traffic in its filters and have the port map as specified
3. If you want email when in ISDN backup, then ensure you have a fixed IP ISDN dialup and set this address as the secondary MX record (via an A record).

Testing :−

1. Confirm by viewing the profile index that the ADSL profile is active (ALERT LED off)
2. Traceroute to confirm routing via ADSL
3. Remove connection to ADSL, and up to wait 1 minute for ALERT LED to come on
4. Confirm by viewing the profile index that the ADSL profile is not active
5. Traceroute to confirm, routing via ISDN
6. Reconnect ADSL and reconfirm that the filter becomes inactive and ALERT LED off with 1 minute

Emailing to tell you the backup has happened :−

1. Set the log/filter options so that Email is selected for ping−scanning
2. Fill in target email address (and optionally, source email address)
3. Enter mail server address, e.g. 10.0.0.2
4. Click "test" to confirm email can be delivered.
5. If test fails, check Status Log for error message and configure mail server accordingly
6. Adjust email delay/timeouts if required

Next hop :−

Monitoring the ADSL link requires that a specific address is checked regularly using a ping. The ping−scanning and ping−failure features of the FireBrick allow for this, and change a profile accordingly. One issue is what address to monitor.

Using traceroute to some address on the internet (your favourite web site for example), you will see the FireBrick, your ADSL router and a next hop. This is a good candidate for monitoring, and means if your ADSL line goes down, the you will switch to ISDN. However, if your ISP has problems (e.g. their upstream fails) and your ADSL line is actually OK, you may lose internet access and not fall back to ISDN.

Using a later address or an address on the internet would allow you to protect against failures within your ISP, and switch to ISDN. Going too far can be a problem, e.g. picking some web site. If you do this, you would find you switch to ISDN simply because the one site you were monitoring was down, even though the rest of the internet was fine.

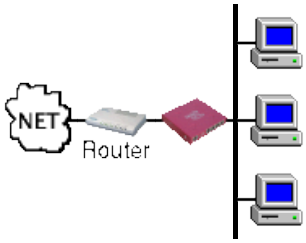
Your ISP may be able to suggest an address to be monitored like this, and this is the best one to use.

1. Check the address you pick answers a ping
2. Make sure nobody minds you monitoring the address − if it is the router next hop, then this is likely to be fine, but some address on the net may upset the owner of that machine. The pings are very light load, but that can be detected.
3. Bear in mind the address could go away. Again, the router next hop is unlikely to, but any other address could be removed or changed without warning. So check you are not using backup routing when you don't want to − we suggest the email alerts are used but keep an eye on the ISDN router just in case.

This example equally applies to :−

1. Any installation with a router and a single subnet
2. e.g. BT net start lines

Cable modem, with one machine having external address



Cable modem/router allocating DHCP addresses
Internal machines on private addresses
One machine set to have cable modem allocated address
NAT for other machines

In this configuration there is a cable modem allocating a single address by DHCP. This is normally intended for use with one PC (so check if terms and conditions allow for use of a network).

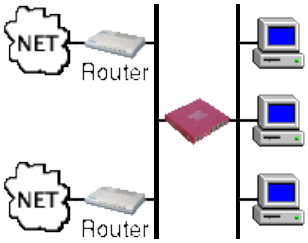
The FireBrick will obtain an address from the cable modem, and provide NAT to a private address block on the inside of the network. PCs on the inside are allocated addresses by DHCP.

One machine on the inside is to have a public address, so as to allow incoming email, web, etc. This address may change because the cable modem service allocated by DHCP, but with the FireBrick constantly renewing addresses, it is unlikely.

1. Create a WAN subnet, marked DHCP client
2. Create a LAN subnet marked DHCP mirror − give it a name such as "SERVER", and mark it DHCP Restrict
3. Create a LAN subnet on a private address range, e.g. 10.0.0.1 mask 24 (255.255.255.0) and set DHCP server addresses (e.g. 10.0.0.10 to 10.0.0.99), and mark as NAT
4. Create a portmap, WAN to FireBrick mapped to LAN with nothing else filled in
5. Ensure the server PC has a name, such as "SERVER" which is the same as the first LAN subnet
6. Adjust filters as required

You should find the WAN subnet gets an address, and the gateway and DNS server addresses are set up automatically.
The LAN subnet should claim to be an address (the gateway address) and allocating a single DHCP address (the WAN address). Using DHCP restrict ensures this will only be issued to a machine called "SERVER".
The PC called SERVER should be set to collect IP automatically (DHCP), and should get the FireBricks WAN address allocated to it on the LAN
The port map ensures the FireBrick will pass on packets from the internet to the internal PC.
Other PCs get private addresses by DHCP and are NATed.

Multiple ADSL lines using bonded uplink



2Mbs/250Kbs no−NAT ADSL line with block of IPs
500Kbs/250Kbs no−NAT ADSL line with block of 4 IPs

In this configuration a customer has a no−NAT 2Mb/s ADSL line (with 250Kb/s uplink) and a large block of IPs so that machines on the LAN have real addresses. The 2Mb/s ADSL is normally used, and the 500Kb/s ADSL is a backup and to provide additional uplink capacity.

- 2Mb/s ADSL router has an address A
- FireBrick allocated an address on 2Mb/s router subnet, address B
- 500Kb/s ADSL router has an address C
- FireBrick allocated an address on 500Kb/s router subnet, address D
- Network adderss for 2Mb/s ADSL line is address E

Basic IP setup :−

1. First subnet, LAN, no NAT, no Stealth, using address B. This gives machines on the LAN real addresses on 2Mb/s line
2. Second subnet, WAN, no NAT, Stealth, using address B. This allows the FireBrick to see router on address A
3. Third subnet, WAN, no NAT, no Stealth, using address D. This allows the FireBrick to see router on address C
4. Routing entry, LAN to WAN for address A, proxy ARP. This allows machines on the LAN to see router address A
5. Equipment on the LAN to use the 2Mb/s ADSL subnet's addresses and FireBrick address B as their gateway.

This basic setup allows machines on the LAN to have real addresses.

Gateway setup :−

1. Default gateway set to address E
2. Gateway alternative list set to addresses A and B

This means that all traffic from to the internet will use the pseudo address E, which is mapped to A and B alternatively for each packet allowing a bonded uplink of 500Kb/s for outgoing traffic. The pseudo address is used because if the router address such as A was used, then the profile based re−routing to use teh 2Mb line would using gateway A would still be mapped to both gateways which would not work if one was down. By using a pseudo address, this is avoided and you can route to A, C or both (using E) based on routing rules as necessary.

Fallback setup :−

1. Profile (2MBADSL) monitoring an internet address, such as routers WAN address, via address A on WAN, set to alert when inactive and reroute on change
2. Profile (500KADSL) monitoring an internet address, such as routers WAN address, via address C on WAN, set to re−route.

3. Add route between subnets and gateway Any−>WAN, gateway A, profile Not 500KADSL
4. Add route between subnets and gateway Any−>WAN, gateway C, profile Not 2MADSL with NAT

This means if the 500K ADSL fails, the default route changes to A and traffic continues only via 2Mb ADSL.
If the 2Mb ADSl fails, the default changes to C and traffic continues via the 500Kb/s ADSL but NATed to ensure replies arrive.

Email alerts of profile changes are recommended.

If you have SMTP incoming email, then you may want to set FireBrick address D as an additional lower priority MX record target, and have a port map for this address to your mail server allowing incoming mail even if the main 2Mb link fails.