HotBrick VPN 6000 user manual

version 193 (2005-01-20)

Title: HotBrick VPN 6000 user manual
Author: Martijn Bakker
Revision: 193 (05-01-20)

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of the publisher.

Microsoft® and *Windows*® are trademarks of Microsoft Corporation in the United States and other countries.
Apple® and *Mac OS*® are trademarks of Apple Computer, Inc., registered in the U.S. and other countries.

Table of Contents

1 Installation.....5
1.1 Requirements.....5
1.2 Getting to know your HotBrick VPN 6000.....5
1.2.1 Front.....5
1.2.2 Back.....5
1.3 Hardware installation.....5
1.4 Connecting to the management interface.....6
1.4.1 Configure a notebook or PC to use DHCP.....6
Enabling DHCP using Windows® 2000.....6
Enabling DHCP using Windows® XP.....10
Enabling DHCP using Mac OS® X.....12
1.4.2 Log in on the firewall management interface.....14
1.5 Entering a valid product key.....15
1.6 Running the “Quick install” wizard.....18
1.6.1 Setting up your LAN connection.....18
1.6.2 Setting up your default internet connection.....21
Setting up WAN1 using DHCP.....22
Setting up WAN1 using a Static/Nat connection.....22
Setting up WAN1 using a PPTP or PPPoE connection.....23
1.6.3 Setting up your fallback internet connection.....23
1.6.4 Confirming and applying results.....24
1.6.5 Connecting to the firewall's management interface.....25
1.7 Backup sets.....26
1.8 Changing the administrator's password.....28
1.9 Setting the firewall's time and date.....30
1.10 (Optionally) disable the firewall's DHCP server.....31
1.11 Connecting LAN and WAN cables.....32
1.12 Errors and recovery.....33

1 Installation

1.1 Requirements

To insure a smooth installation of your HotBrick VPN 6000, we should make sure to have all the necessary equipment and information ready. To configure your firewall for the first time we will need:

1x HotBrick VPN 6000

1x Standard power cord (bundled with HotBrick VPN 6000)

2x UTP RJ45 cables (bundled with HotBrick VPN 6000)

1x PC or notebook computer

1x HotBrick VPN 6000 license key

If we are to set up your firewall to handle one or more Internet connections, we will also need:

Connection details provided by your Internet Service Provider (ISP)

1.2 Getting to know your HotBrick VPN 6000

1.2.1 Front

1. LCD display
2. Serial port
3. WAN1 port
4. WAN1 connection LED
5. WAN2 port
6. WAN2 connection LED
7. FLEX1 port
8. FLEX1 connection LED
9. FLEX2 port
10. FLEX2 connection LED
11. FLEX3 port
12. FLEX3 connection LED
13. FLEX4 port
14. FLEX4 connection LED

1.2.2 Back

15. Power socket
16. Power switch
17. More??

1.3 Hardware installation

➔ Use the power cord to connect the HotBrick VPN 6000's power socket (15) to a standard wall power outlet.

➔ Switch the firewall on, using the power switch (16), on the back of the device.

Booting the hardware for the first time may take up to 1 minute.

When the firewall is switched on and ready, you should hear 3 short beeps. If you have not heard 3 beeps within 1 minute of switching on the device, please refer to section 1.12 (Errors and recovery).

➔ Use an UTP RJ45 cable to connect the firewall's FLEX1 port (7) to a network connector on your PC or notebook.

➔ Switch on the PC or notebook.

The FLEX1 connection LED above the FLEX1 port (8) should come on. If this LED does not come on, please refer to section 1.12 (Errors and recovery).

1.4 Connecting to the management interface

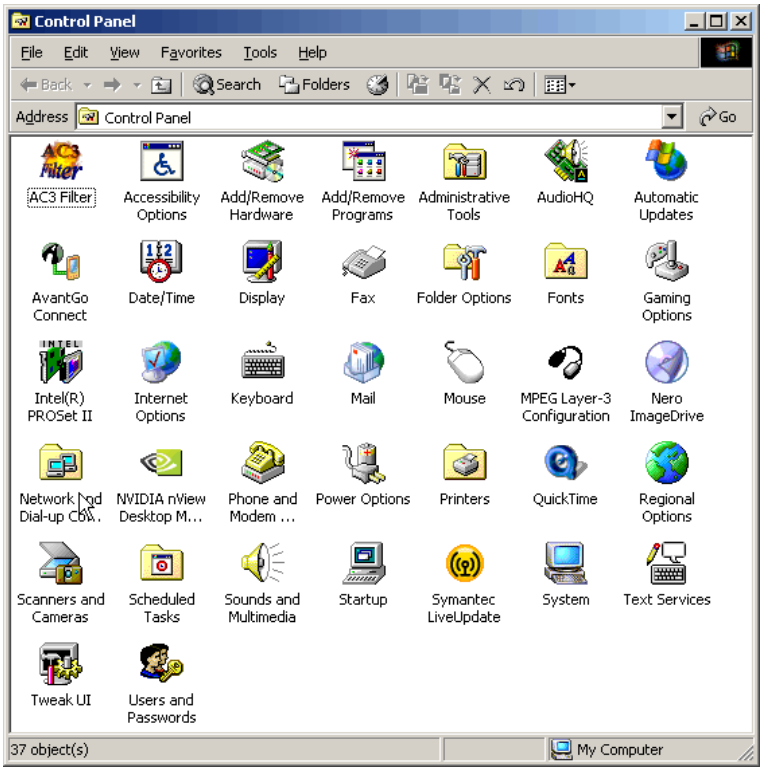
Your HotBrick VPN 6000 is highly configurable by means of a powerful management interface. Once the device is properly set up you will be able to access this interface from any machine in your local network (provided you know the right password). For the initial setup of the firewall we will make use of the same management interface. However, because the device is not set up to connect with a local network or Internet connection, it must first be configured using a single PC or notebook.

1.4.1 Configure a notebook or PC to use DHCP

If you are to use the firewall's management interface from your notebook or PC, then both are to be connected and using a common network setup. The fastest way to effect this is to have your PC or Notebook computer configure it's network settings automatically by means of DHCP (Dynamic Host Configuration Protocol). As this is done in a slightly different manner by various operating systems, the following sections will detail the procedure for enabling DHCP in *Windows*® 2000, *Windows*® XP (or *Windows*® 2003) and *Mac OS X*® respectively.

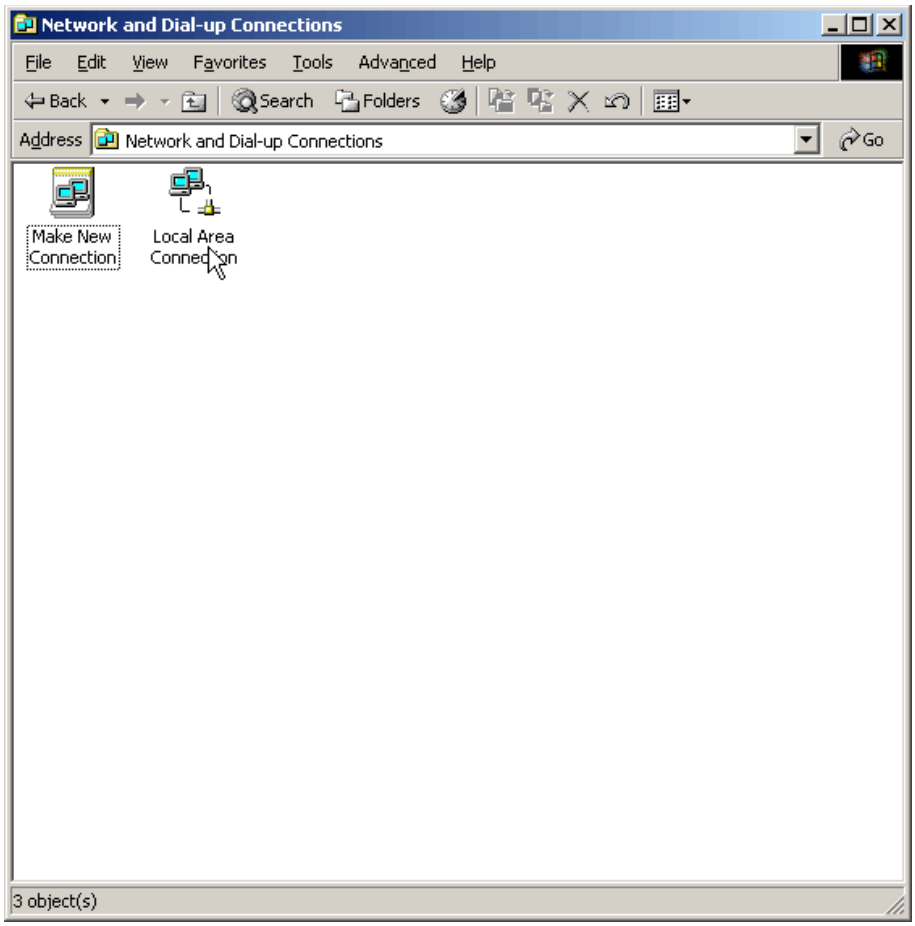
Enabling DHCP using Windows® 2000

➔ Using the *Windows*® "Start" menu (and Settings sub menu), open the "Control Panel".



➔ In the “Control panel”, double click the “Network and Dial-up Connections” icon.

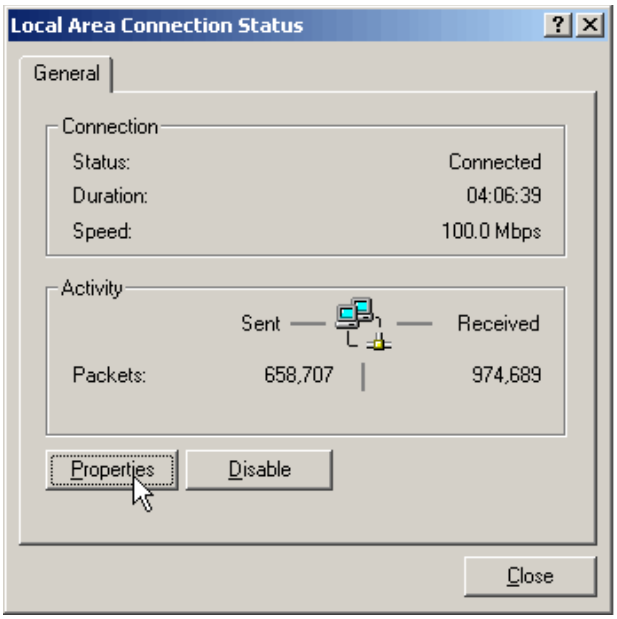
The window “Network and Dial-up Connections” should open.



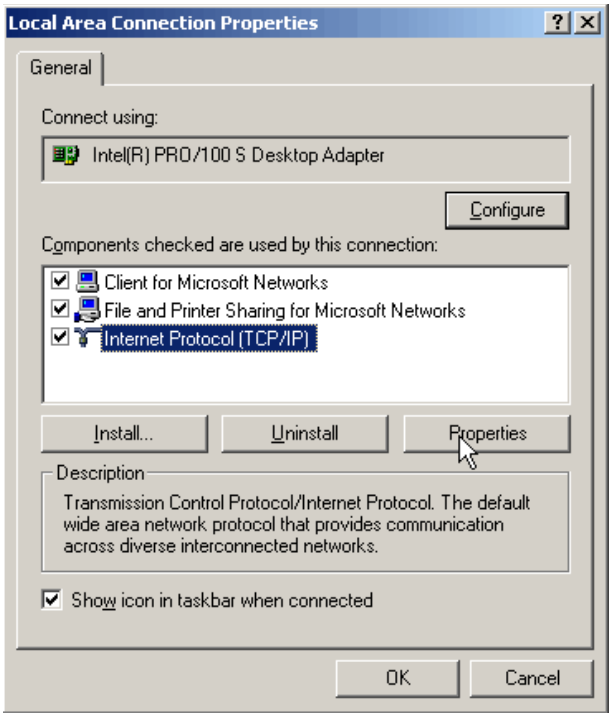
➔ In the “Network and Dial-up Connections” window, double click the “Local Area Connection” icon.

The “Local Area Connection Status” window should open.

➔ In the “Local Area Connection Status” window, click the “Properties”button.



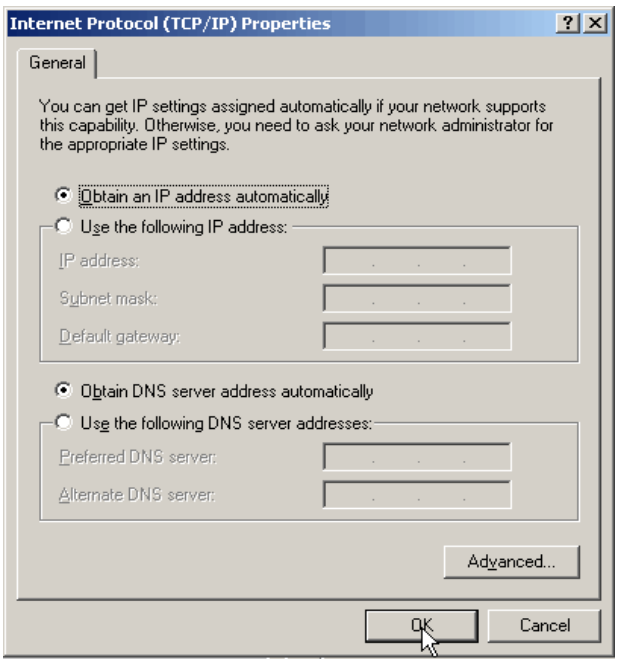
The “Local Area Connection Properties” window should open.



➔ In this window, select “Internet Protocol (TCP/IP)” (the blue line in the example below).

➔ Click the “Properties” button.

The window “Internet Protocol (TCP/IP) Properties” should open.



➔ Make sure settings in this window are as specified in the example above (check “Obtain an IP address automatically” and “Obtain DNS server address automatically”.

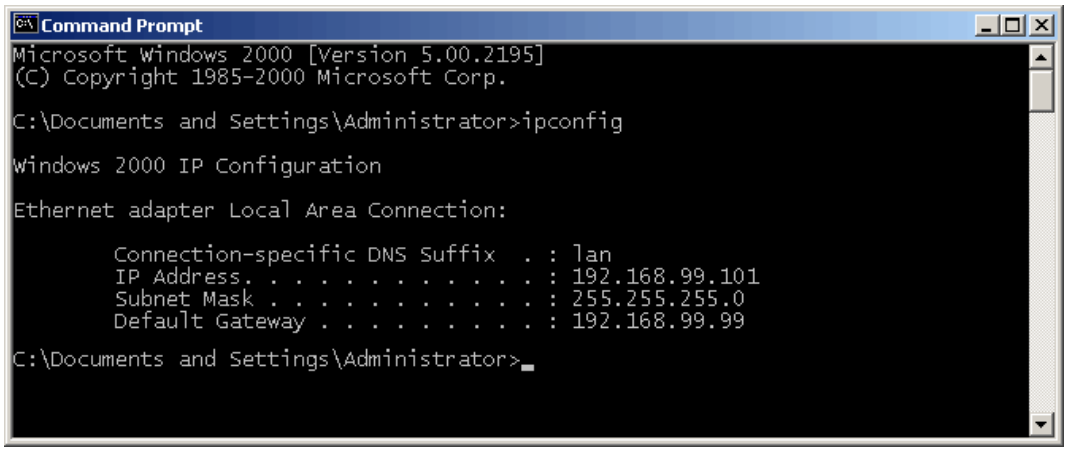
➔ Click the “OK” button to confirm your changes.

➔ To verify your settings, open a “Command Prompt” (From the “Start” menu, through “Programs”, in the “Accessories” sub menu).

➔ In the command prompt type:

```
ipconfig
```

The output should look like this:



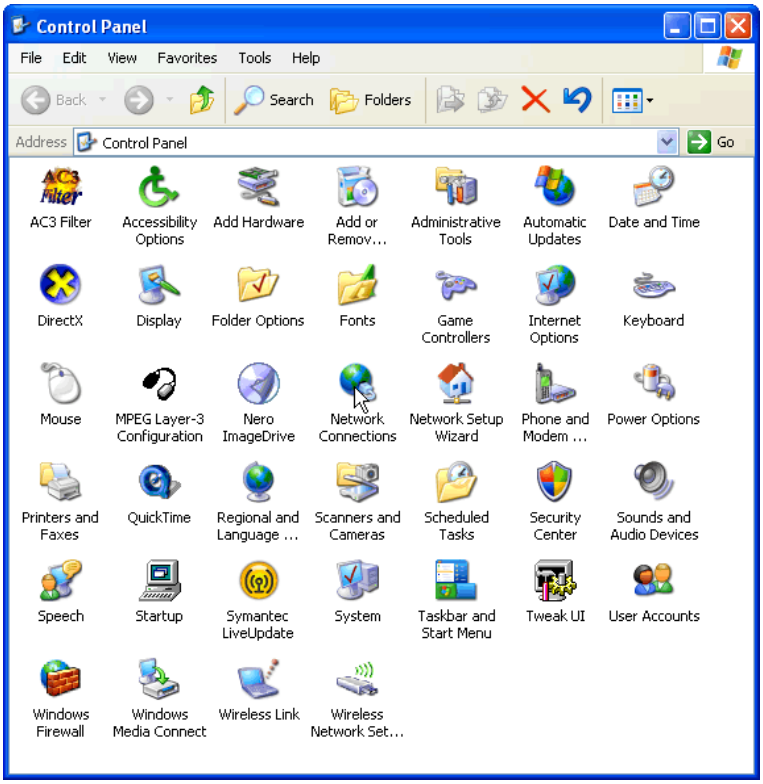
➔ If the “IP Address” line does not list an address starting with 192.168.99, please try typing:

```
ipconfig /renew
```

This should force the PC or Notebook to request a new network address. If you still fail to get an “IP Address” in the correct range, please refer to section 1.12 (Errors and recovery).

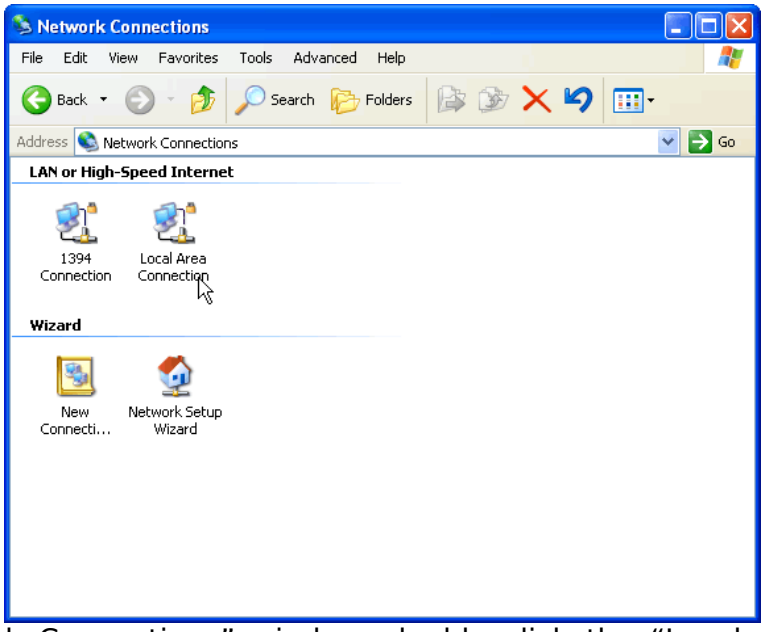
Enabling DHCP using Windows® XP

➔ Using the *Windows*® “Start” menu (and Settings sub menu), open the “Control Panel”.



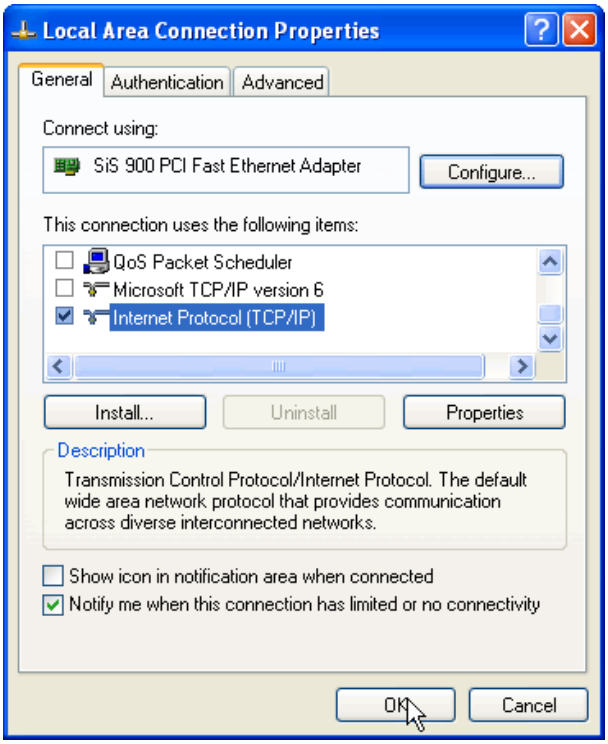
➔ In the “Control Panel”, double click the “Network Connections” icon.

The “Network Connections” window should open.



➔ In the “Network Connections” window, double click the “Local Area Connection” icon.

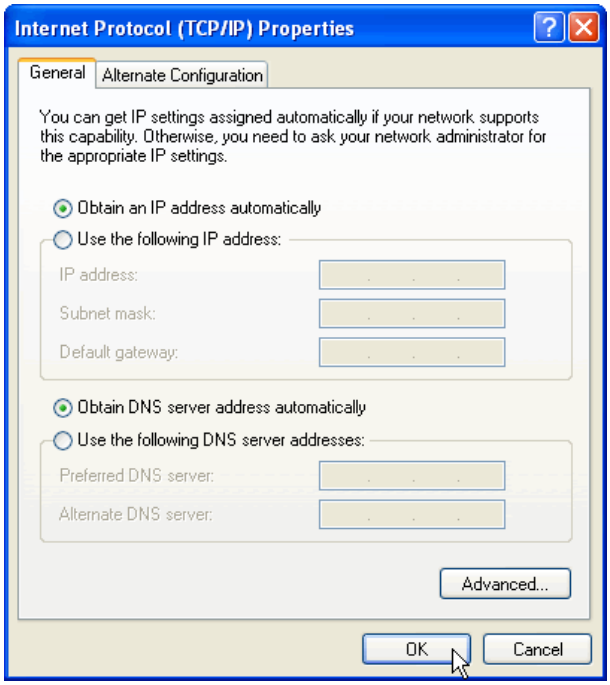
The “Local Area Connection Properties” window should open.



➔ In the “Local Area Connection Properties” window, select “Internet Protocol (TCP/IP) ” (the blue line in the above example).

➔ Then press “Properties”.

The “Internet Protocol (TCP/IP) Properties window should open.



➔ In the “Internet Protocol (TCP/IP) Properties” window, make sure settings are as in the above example (“Obtain an IP address automatically” and “Obtain DNS server address automatically”are selected).

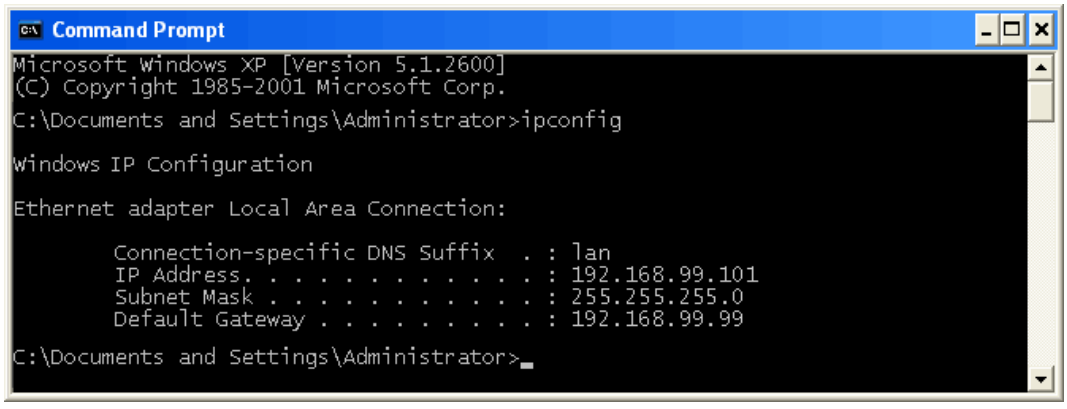
➔ Press the “OK” button to confirm your new settings.

➔ To verify your settings, open a “Command Prompt” (From the “Start” menu, through “All Programs”, in the “Accessories” sub menu).

➔ In the command prompt type:

```
ipconfig
```

The output should look like this:



➔ If the “IP Address” line does not list an address starting with 192.168.99, please try typing:

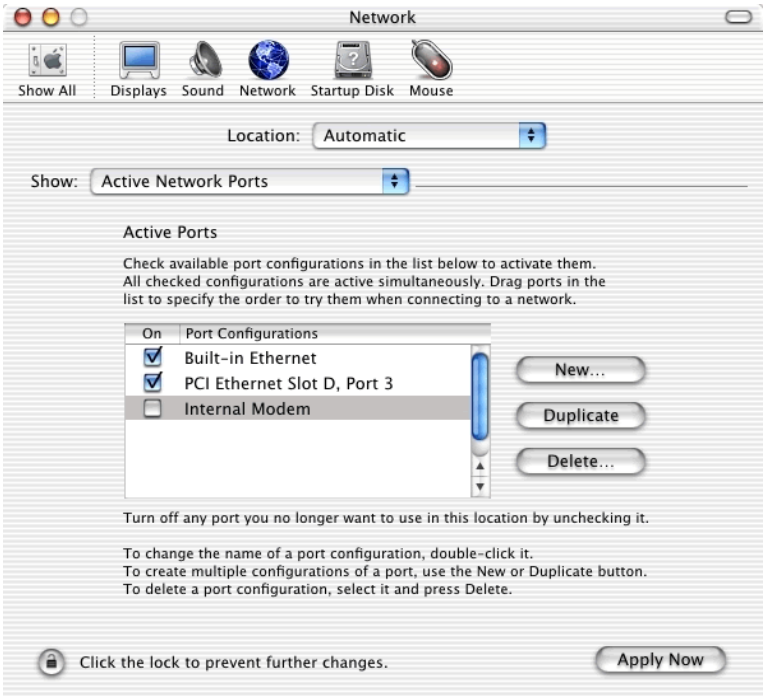
```
ipconfig /renew
```

This should force the PC or Notebook to request a new network address. If you still fail to get an “IP Address” in the correct range, please refer to section 1.12 (Errors and recovery).

Enabling DHCP using Mac OS® X

➔ From the *Apple*® menu, choose “System Preferences”, then “Network”.

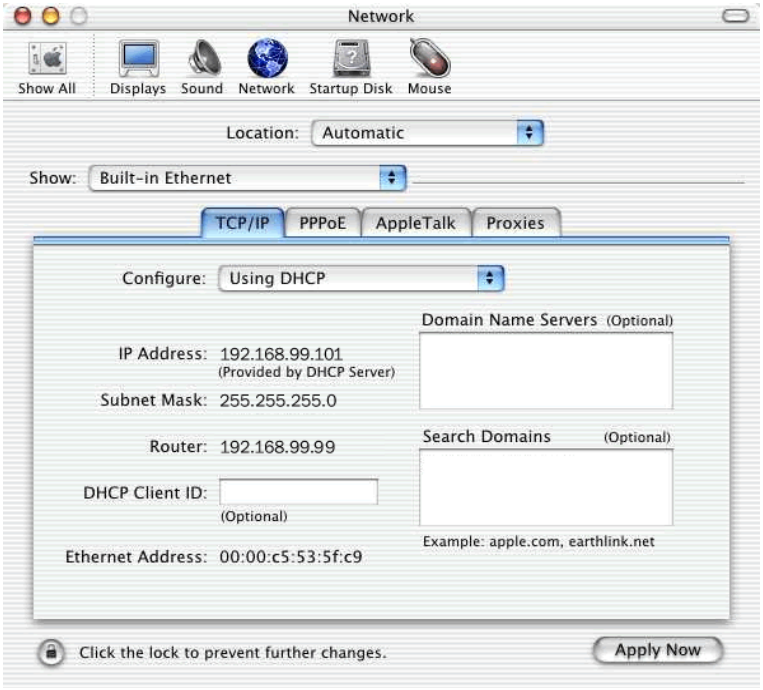
The Network window should open.



➔ In the “Network” window, make sure the “Show” box is set to show “Active Network Ports”.

➔ Drag “Built-in Ethernet” to the top of the list.

➔ Set the “Show” box to “Built-in Ethernet”.



➔ Now select the “TCP/IP” tab.

➔ Switch the “Configure” box to “Using DHCP”.

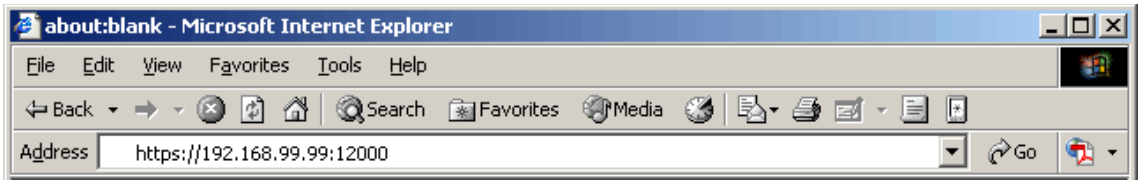
➔ Verify that the “IP address”, “Subnet Mask” and “Router” settings are as shown (192.168.99.101, 255.255.255.0 and 192.168.99.99 respectively).

➔ Click “Apply Now” to confirm your changes.

1.4.2 Log in on the firewall management interface

➔ Open a web browser on the PC or Notebook you have just configured

➔ Enter the address “ https://192.168.99.99:12000”into the address bar.



➔ When prompted for a user name and password, enter “admin” (user name) and “password” (as password).

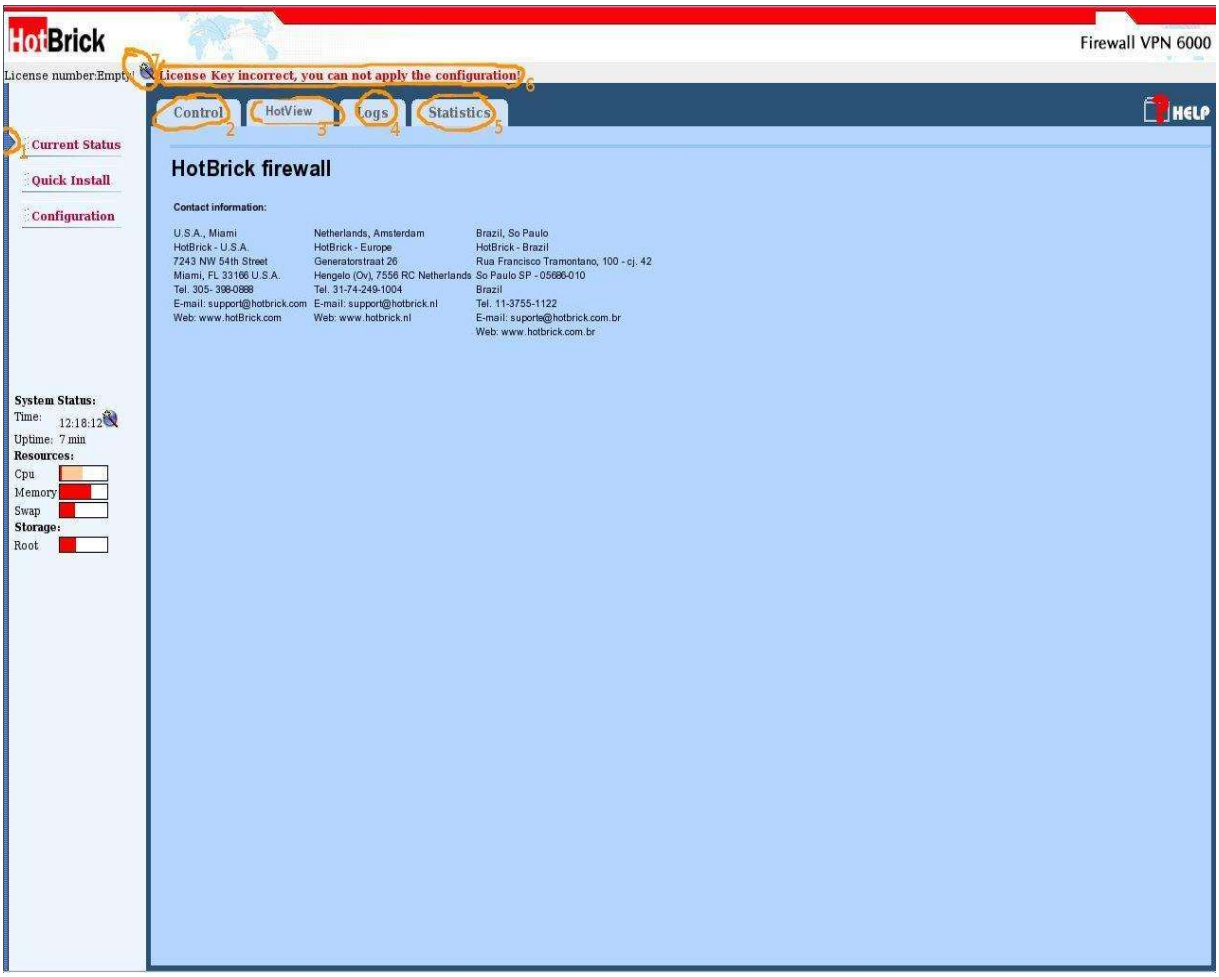
➔ Click “OK”.

If you get a “timeout”, “not found” or “permission denied” error, please refer to section 1.12 (Errors and recovery).

1.5 Entering a valid product key

The factory defaults of your HotBrick VPN 6000 do not contain it's product key. Without the product key, none of the changes you make in the firewall's management interface can be applied. Therefore, it is essential that the very first thing we do after establishing a connection is entering a valid product key.

Once you have logged in to the firewall's management interface, you should see the following welcome screen.



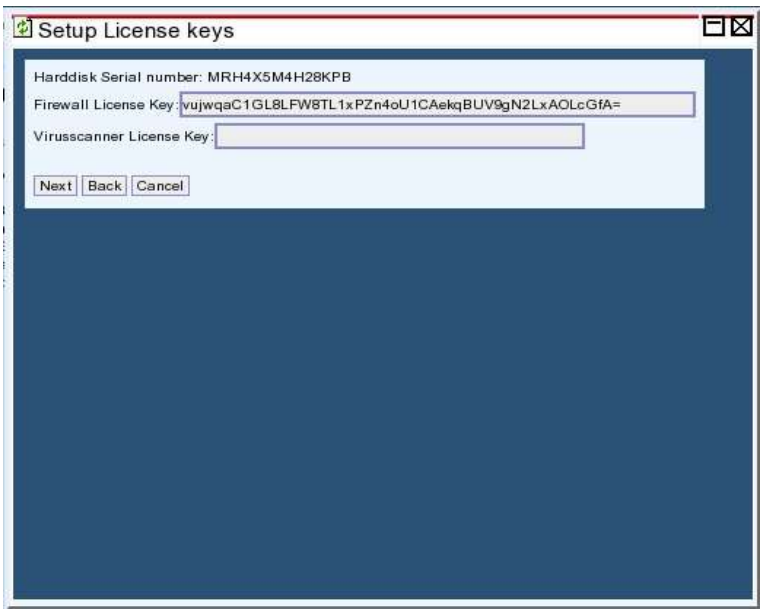
A blue triangle in the upper left-hand corner of the screen indicates we are looking at the “Current Status”(1) of the firewall. Tabs labeled “Control”(2), “HotView”(3), “Logs”(4) and “Statistics”(4) provide access to other screens in the “Current Status” context. The red warning message at the top of the screen (5) indicates the current lack of a valid license key.

The system status on the left hand side of the screen, about half-way to the bottom displays some statistics concerning the operation of your firewall's hardware. These statistics are updated once every 10 seconds, to insure the accuracy of the information.

Immediately left of the red warning text, in the upper left-hand corner of the screen is an icon of a globe, fronted by a magic wand (6).

➔ Click this icon (7) to enter your license key.

The “Setup License Keys” dialog window appears.



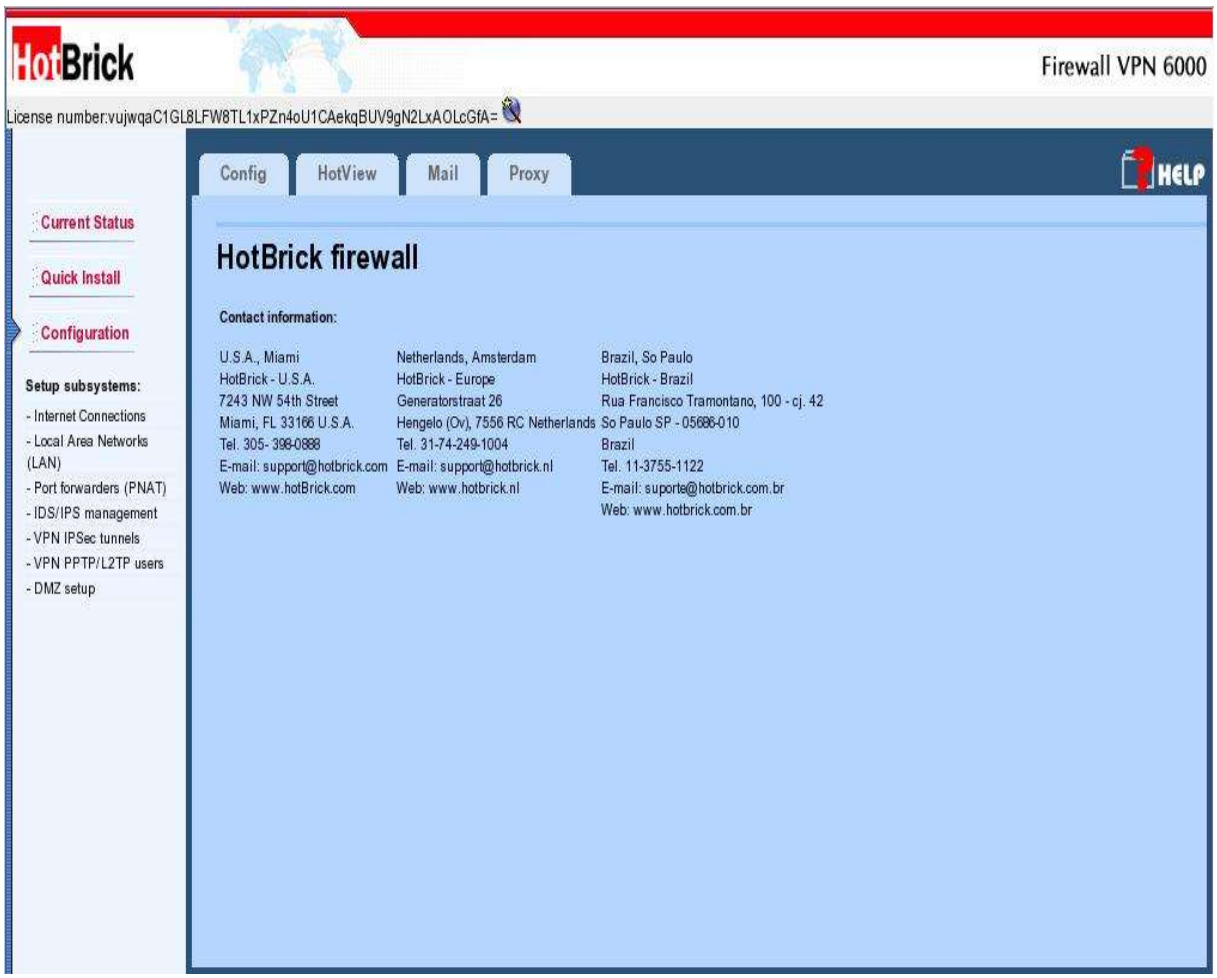
➔ Enter the license key provided with your HotBrick VPN 6000.

➔ Press “Next” to continue.

If you entered the license key correctly, the next window should allow you to confirm the changes and return to the firewall management interface.

If you have incorrectly entered a license key, you will be asked to enter the license key again. If the license key should fail repeatedly, the license key may not match your hardware. Please refer to section 1.12 (Errors and recovery).

After confirming your entered license key, you will see the following screen:



Note the license key in the top left corner of the screen (now in black). The blue triangle in the left of the screen indicates we are now looking at the “Configuration” context. This has slightly different tabs from the “Current Status” context we saw before (namely “Config”, “HotView”, “Mail” and “Proxy”).

The “Current Status” context will display information concerning the status of your device, while we will use the “Configuration” context to make changes to it's intended behavior.

The “Configuration” context has a number of “wizards” available, that can be used to provide assistance performing common tasks. The list of wizards is found on the left hand side of the screen, right below the red “Configuration” text. They are “Internet Connections”, “Local Area Networks”, “Port forwarders (PNAT)”, “VPN IPSec tunnels”, “VPN L2TP/PPTP users” and “DMZ setup”. The “Quick install” wizard is not listed here. Instead, we start the “Quick install” wizard by clicking the red “Quick Install” text, between the “Current Status” and “Configuration” context indicators.

The next step in setting up your HotBrick VPN 6000 is running the “Quick install” wizard.

1.6 Running the “Quick install” wizard

The “Quick install” wizard was intended to allow you to quickly and efficiently tailor the HotBrick VPN 6000 to match your network's needs and settings. Whenever you start a “Quick install” wizard, all current configuration data will be lost.

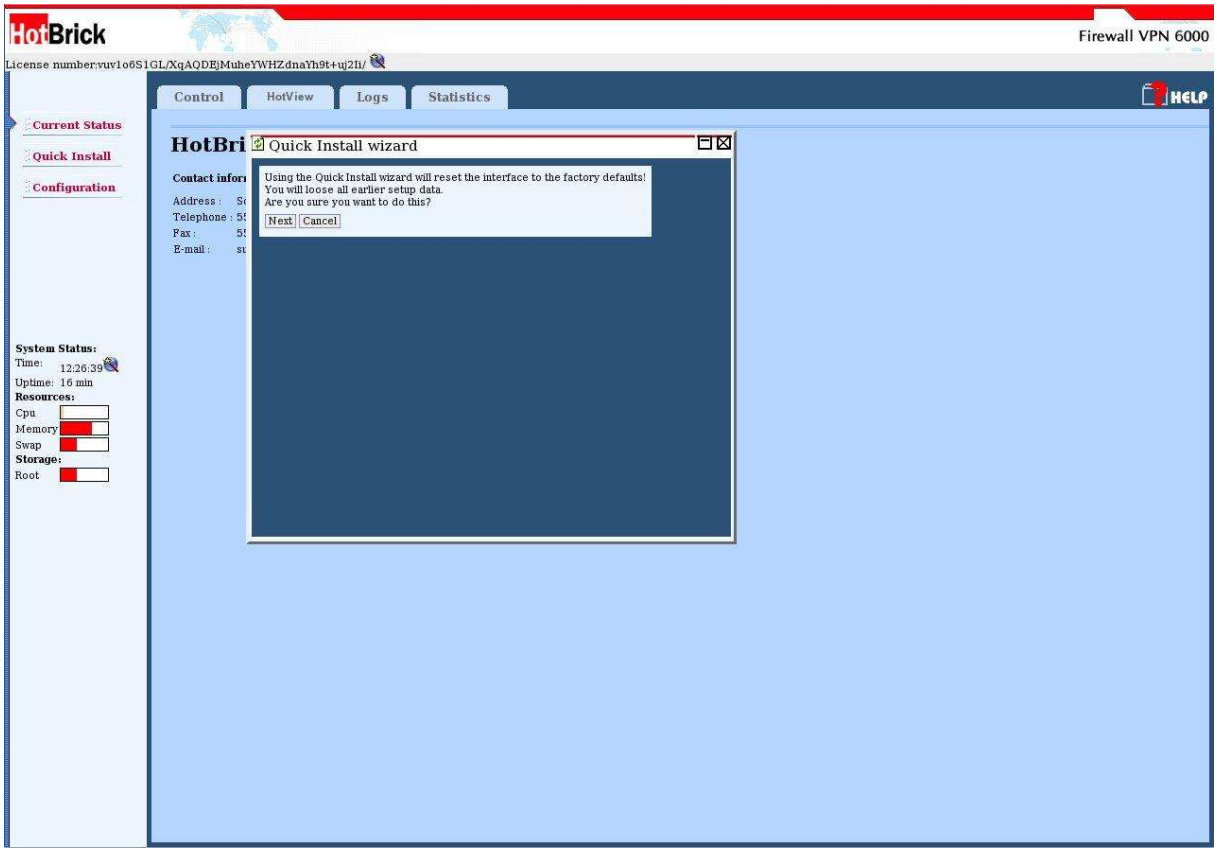
At a first installation this should not pose a problem. However, if you ever feel you should change important configuration data at a later stage, you are encouraged to use the “Local Area Networks” or “Internet Connections” wizards from the “Configuration” context instead.

You may start the “Quick install” wizard by pressing the red “Quick install” text, in the left hand side of the screen, between “Current Status” and “Configuration”.

➔ Start the “Quick install wizard”

When you start the “Quick install” wizard, a warning screen signals the start of this wizard. The screen is there to prevent you from inadvertently starting the “Quick install” wizard at a later time, thereby deleting all your current network settings. However, for a first install, we do not consider this a problem.

➔ Click “next”.



1.6.1 Setting up your LAN connection

The first step after starting the wizard is to set up your LAN (Local Area Network) connection. This is the connection between the firewall and your local network. As a firewall, the HotBrick VPN 6000 should serve as a buffer between your Internet

connections (WAN or Wide Area Network connections) and your local network (or LAN).

The “Quick Install” wizard will allow you to enter network settings specific to your local network. First we enter a label to use for the local network. Default setting is “lan”, which seems sensible. In more complex network environments, with more than one LAN you may opt to use a more descriptive name (like “public lan” or “accounting lan” instead). In any case, make sure the names you use are unique throughout your organization, to avoid confusion arising from identical network names for different networks.

➔ Enter a network name for your local network

The next values to enter are an internal IP Address for the firewall (in the context of the LAN) and a net mask. Together, the IP Address and the net mask define a network address for the local network. In our example we use an IP Address of 192.168.0.1, with a net mask of 24 (bits). A net mask of 24 (=3*8) means that the first three numbers from the IP Address will be part of the network address, so all addresses in the network start with 192.168.0. If you already have a local network, then this network address should have a predefined value (if uncertain, contact your network administrator). In this case, please note that HotBrick VPN 6000 displays the net mask as a number of bits, not in the 255.255.255.0 format.

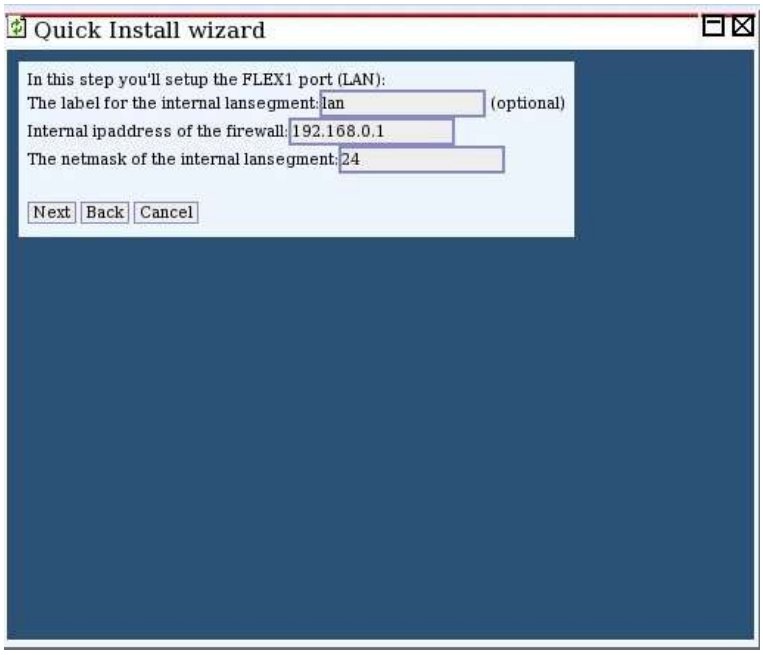
If you do not have a local network, then you need to pick an address for your local network first. There are a number of possible network addresses set aside for use in a local network. The table below lists the possible IP addresses, their net masks and uses:

Firewall IP address	***Net mask***	***Network Address***	***Internal IP addresses***	***maximum addresses***
192.168.x.z	24	192.168.x.0	192.168.x.n	254
172.16.x.z	24	172.16.x.0	192.168.x.n	254
10.x.y.z	8	10.0.0.0	10.n.m.p	16 million

Where x, y can denote any *predefined* number between 0 and 255, z can denote any predefined number between 1 and 254, while n, m and p may be any number between 1 and 254.

Generally, a local network does not need over 254 IP addresses (per distinct local network). We would therefore recommend you choose a 192.168.x or 172.16.x network.

Users who intend to use the HotBrick VPN 6000 to connect their local network to another LAN by means of a VPN tunnel (or indeed, anyone wishing to leave this option open) will do well to choose a different network address for each LAN (for example 192.168.0.0, 192.168.1.0, 192.168.2.0 etc.).



As an example only, we will make use of a 192.168.0.0 network in this user manual. We will set the firewall's internal IP address to 192.168.0.1 and the net mask value to 24 (as befits a 192.168.x.0 network).

➔ Enter a firewall IP address.

➔ Enter the corresponding net mask.

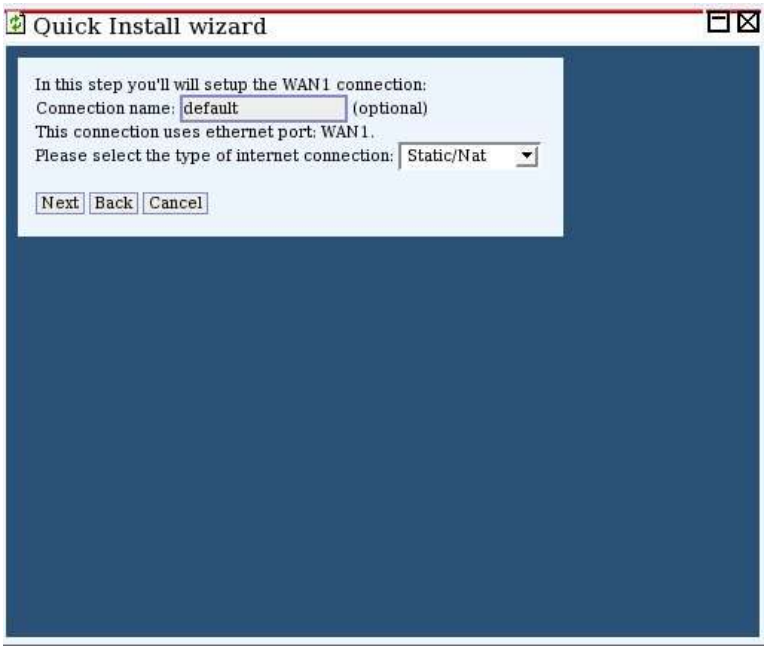
➔ Write down the IP address and net mask values for later reference.

➔ Click “next” to continue

1.6.2 Setting up your default Internet connection

The next step in the wizard is to set up your WAN (Wide Area Network) connections. These are your connections to the Internet. The HotBrick VPN 6000 allows for two WAN connections, one default connection and one fall back. The default connection we name WAN1 (and we will eventually connect the modem or router to the WAN1 network port). The fall back connection we name WAN2 (and like with WAN1, the modem or router for this network connection, if any, will be connected to the WAN2 port).

First we will setup your WAN1 Internet connection.



In this screen we can enter a name for the WAN1 (default) Internet connection. Per default, this name is set to “default”. (WAN2 is named “fall back” per default). Any name can be entered here. You are encouraged to use a descriptive name for the Internet connection. For example “MyISP DSL” or “AOL dial in”. This way, it will be easier to tell two separate Internet connections apart in the future.

➔ Enter a “Connection name” for your default Internet connection.

The type of Internet connection to choose is slightly more complicated. Different types of Internet connections will require different values. As a consequence, the next screen in the “Quick install” wizard will look slightly different, based on the choice you make here.

If you have an Internet connection by means of an ISDN router or a cable or DSL modem, you will generally be able to choose “DHCP”. Choosing “DHCP” is the easiest possible configuration. Choosing DHCP will allow you to skip the next screen in the “Quick install” wizard entirely. You do not have to enter any connection details as these can be automatically configured.

However, when you have a routed subnet or a fixed IP address for your Internet connection and have been provided with an IP address, a net mask and a standard gateway address by your Internet service provider (ISP), please choose “Static/NAT”

instead. Be sure to have the connection details provided by your ISP at hand, because you will need these in the next screen.

Some Internet providers may have you authenticate before connecting to the Internet, preferring to use PPTP or PPPoE. If you have such a connection, choose “PPTP/PPPoE”. Like with a Static/NAT connection, setting up a PPTP/PPPoE Internet connection will require connection details provided by your ISP.

When in doubt about the type of Internet connection to choose, please contact your ISP.

➔ Select the type of Internet connection appropriate to your situation.

➔ Press “next” to continue.

Setting up WAN1 using DHCP

The easiest way to connect WAN1 to the Internet is using DHCP. Generally, when choosing DHCP, no further settings are required for an Internet connection. After pressing “next” you will directly be offered the opportunity to set up your WAN2 interface (fall back Internet connection).

Setting up WAN1 using a Static/Nat connection

When using a single static IP address or a routed subnet for your network connection, you will have been provided with an IP number, a net mask and a default gateway by your ISP. After choosing “Static/Nat” as type of Internet connection, the next screen will offer the opportunity to enter this data.

➔ Enter the IP address, net mask and gateway address.

If you are in any way unsure about the correct number to enter, please contact your ISP for confirmation.

Setting up WAN1 using a PPTP or PPPoE connection

PPTP or PPPoE Internet connections are not identical, but since both require user authentication, the options to enter are much the same.

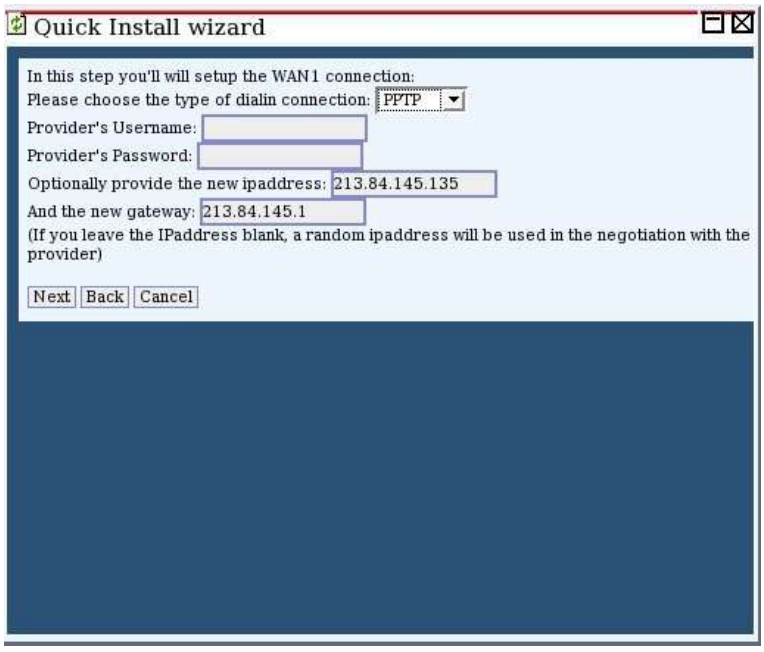
➔ Enter the type of Internet connection (PPTP or PPPoE) after the text “Please choose the type of connection”.

(in the example screen below, we use PPTP. Please remember that this procedure also applies for PPPoE connections).

➔ Enter the user name and password provided by your ISP in the corresponding fields.

If you do not know the correct type of connection, user name and/or password, please contact your ISP for these details.

Some ISP's also require you request a specific IP address of gateway. If such is the case, you can put these values in the *optional* IP address and gateway fields. Most users may simply leave these fields empty.



➔ If required, fill in the “new IP address” and “new gateway” fields

➔ Press “next” to continue.

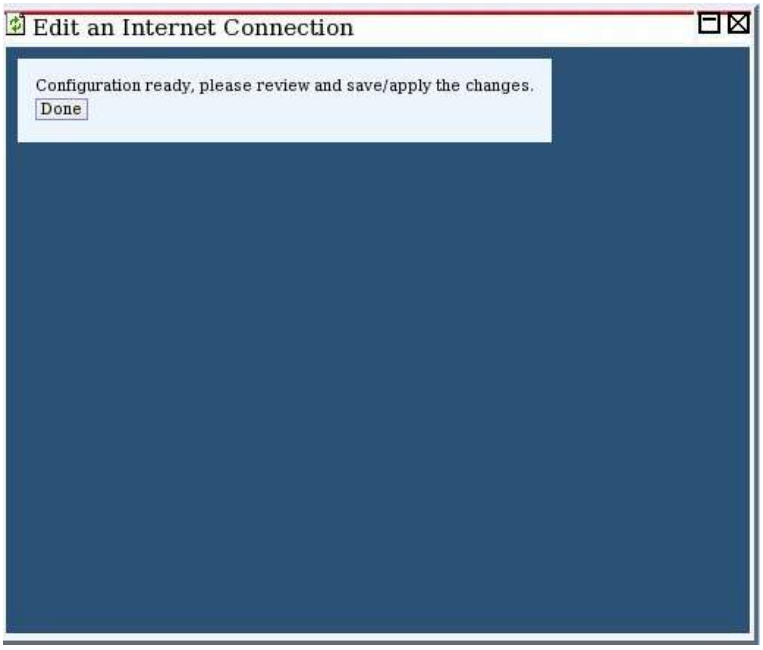
1.6.3 Setting up your fall back Internet connection

Next, you will be asked to set up your fall back Internet connection (WAN2). Setting up a fall back Internet connection is much the same as setting up your default connection (covered in the previous paragraph). Therefore we will not include a detailed description here.

If you do not have a fall back Internet connection, or do not wish to use one, please choose “DHCP” as the type of Internet connection for WAN2. Your firewall will automatically detect the absence of a connection on WAN2 and will not make use of this connection.

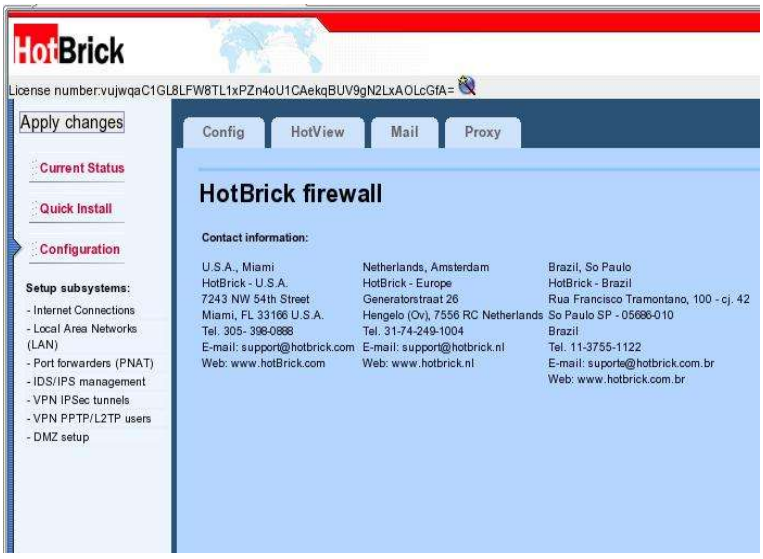
1.6.4 Confirming and applying results

After we have set up our LAN and our default and fall back Internet connections, the “Quick Install” wizard is done.



➔ In the final confirmation screen, click “done” to close the wizard.

The top left-hand corner of the screen of our firewall's management interface should now show the text “Apply changes”. Changes made in the “Quick install” wizard are only made permanent once you click this text.



Please note that when you do this, your firewall's IP address will probably change. Since the IP address of the firewall will change, the address we used to log in to the management interface will no longer point to the firewall. Hence we will lose our connection to the firewall temporarily. To log in to the management interface after applying changes, we will need the firewall's new IP address.

➔ Make sure you have the firewall's new IP address (in the local network) written down.

➔ Click “Apply changes”

If you used the “Quick install” wizard to alter the firewall's IP address on the local network, the we will lose our connection to the firewall after applying changes. The next paragraph deals with re-establishing the connection.

1.6.5 Connecting to the firewall's management interface

After we've applied the changes made in the “Quick install” wizard, we may loose our connection to the firewall's management interface because (according to the firewall's new local network settings) our PC or notebook is no longer on the same local network as the firewall is. If such is the case, then we have to make a new connection to the firewall before we can proceed.

The first step towards this is to obtain a new network address, which is valid according to the firewall's local network settings. A good way to do this is to reboot the PC or notebook. (Experienced system administrators may opt to renew their machine's DHCP lease instead. Remember to verify the addresses you obtain by this method).

➔ Reboot the PC or notebook

➔ After rebooting the computer, start a web browser.

➔ In the address bar of your web browser, type “https://”, followed by the IP address of the firewall (which you have written down), followed by “:12000”. In our example this would lead to the address https://192.168.0.1:12000. Then press enter.

➔ When prompted for a user name and password, enter “admin” (user name) and “password” (as password), then click “OK”.

If you get a “timeout”, “not found” or “permission denied” error, please refer to section 1.12 (Errors and recovery).

1.7 Backup sets

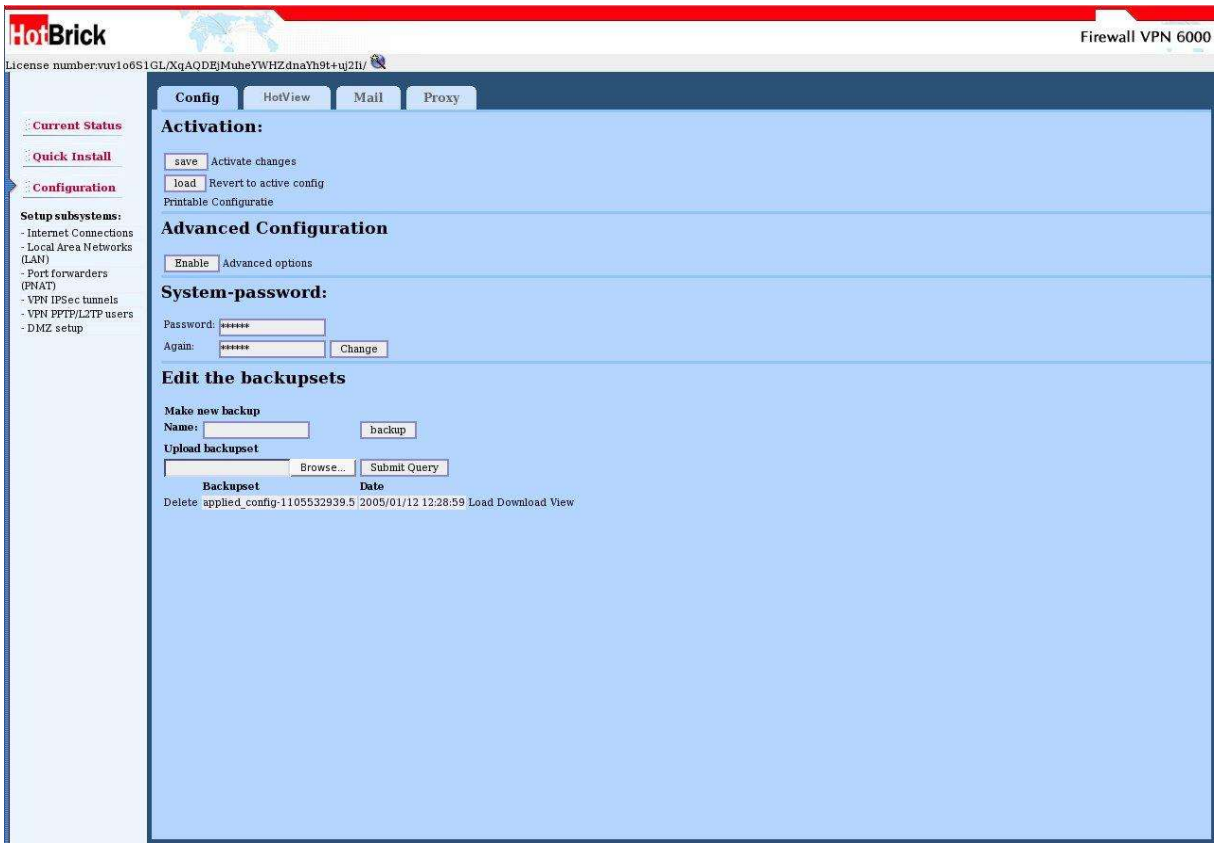
The new settings you've just applied have been stored in the firewall as current configuration, but also as a “backup set”. A “backup set” is a snapshot of the HotBrick VPN 6000's configuration in a single file. These backup sets can be uploaded to the firewall, or downloaded from the firewall. Thus it is possible to send or receive an entire firewall configuration in a single file. You can also store a backup set on another computer or backup medium, as a backup of the HotBrick VPN 6000's configuration.

Operations on backup sets are performed in the “Config” tab of the “Configuration” context.

➔ Click on the red “Configuration” text in the left-hand side of the screen to enter the “Configuration” context.

➔ Activate the “Config” tab by clicking it once.

Under the heading “Edit the backup sets” you will find the stored backup sets as well as buttons for possible operations on the backup sets.



At the moment we have one stored backup set (“applied-config-1105532939.5” in the above example). Pressing “Delete” (before the name of the backup set, on the left), will delete the backup set from the firewall's memory. This will not affect the firewall's current settings, but is still inadvisable. On the right hand side of the backup set's name we find the other options, “Load” (which restores the firewall's configuration to the values stored in the backup set), “Download” (which we can use to download a backup set with the firewalls current settings to our computer) and “View” which gives a summary of firewall settings in the selected backup set.

➔ Click “download” to download a copy of the backup set we've just made to your computer.

Whenever you contact support personnel about a problem with your configuration, they may ask you to send a backup set containing your current firewall settings.

1.8 Changing the administrator's password

No system can be secure using a factory default password. Before we deploy the HotBrick VPN 6000 in a real network environment we therefore advise you change the administrator's password.

A good administrator's password is at least eight characters long, contains letters (preferably in both upper- and lower case) as well as numbers or non-alphanumeric characters. It can not be found directly in any dictionary but should still be memorable to those in the know.

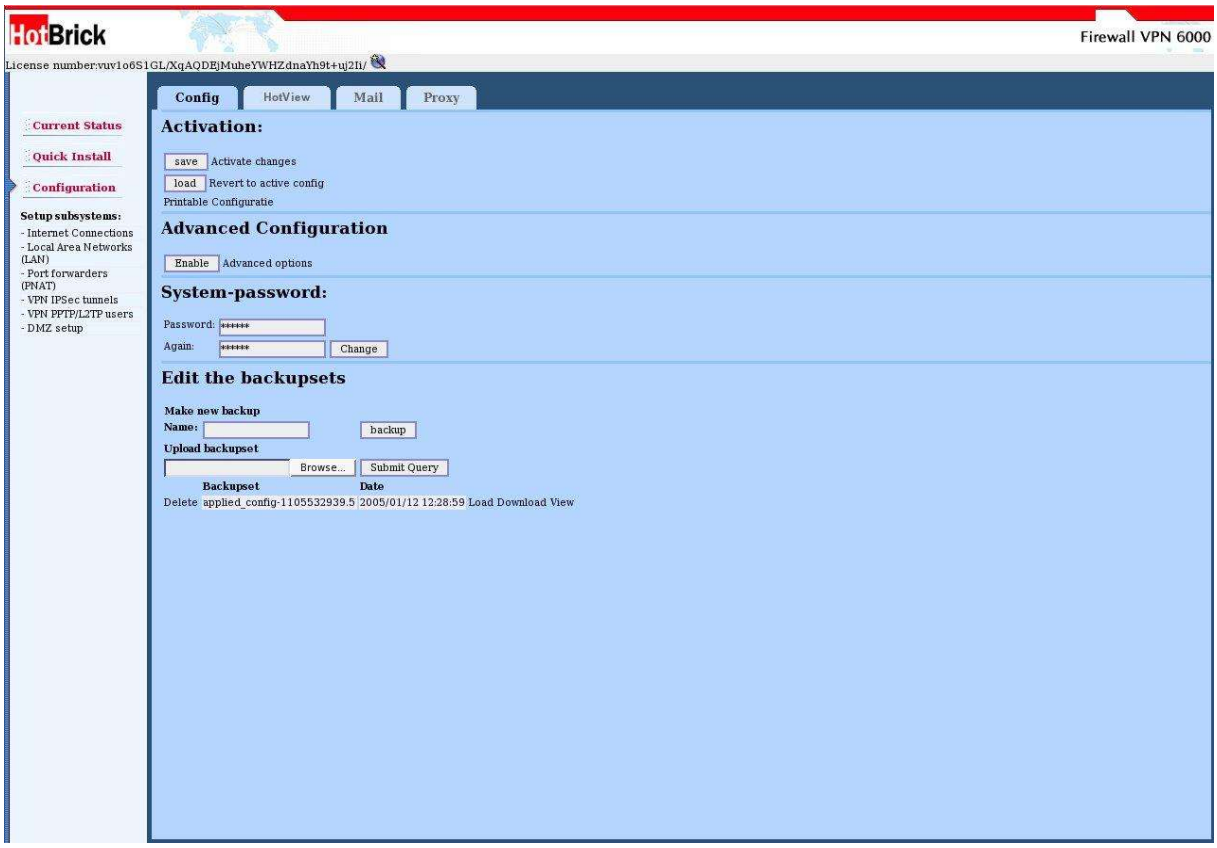
➔ Think up a good administrator password

It is essential that you not forget this password. You will not be able to manage your firewall without it. It is strongly recommended you file at least one copy of your password (in a sealed envelope) to a safe or to your direct superior.

We change the administrator's password from the “Configuration” context.

➔ Click on the red text “Configuration” on the left hand side of the screen to enter the “Configuration” context.

➔ Activate the “Config” tab by clicking it.



➔ Under the heading “System password”, next to “Password”, enter your new administrator's password.

➔ Enter the same password again one line lower (next to Again:).

➔ Click “change” to change the password.

After changing the administrator's password, your own login (based on the previous administrator password) will also expire. It will therefore be necessary to provide a user name and password again before continuing.

➔ Log in with the user name “admin” and the password you have just entered.

1.9 Setting the firewall's time and date

The configuration of your HotBrick VPN 6000 is not fully complete until you have set the correct time and date. It is customary for computers connected to the Internet to use the network time protocol (NTP) to regularly update their date and time.

➔ Click on the red text “Current Status” on the left hand side of the screen to enter the “Current Status” context.

➔ Once in the “Current Status” context, find the current time on the left hand side, about half way to the bottom.

➔ Press the globe and magic wand icon right of the time indicator

The “Setup TimeZone and NTP servers” window will open.

➔ From the “Timezone” menu, choose your timezone.

➔ Enter at least one valid NTP server under “NTP servers:” (for example us.pool.ntp.org)

➔ Click “next” to continue

➔ Click “done” to confirm your changes

Your HotBrick VPN 6000 will now use the Internet connections to keep it's internal clock and calendar synchronized.

1.10 (Optionally) disable the firewall's DHCP server

Per default, the HotBrick VPN 6000 is set to use a DHCP server to automatically configure network addresses of computers in you local network. This could, potentially, cause problems if you have another DHCP server running in your network. Any local network may only contain one DHCP server at a time.

If you wish the HotBrick VPN 6000 to serve as DHCP server, make sure you disable any other DHCP servers in your local network.

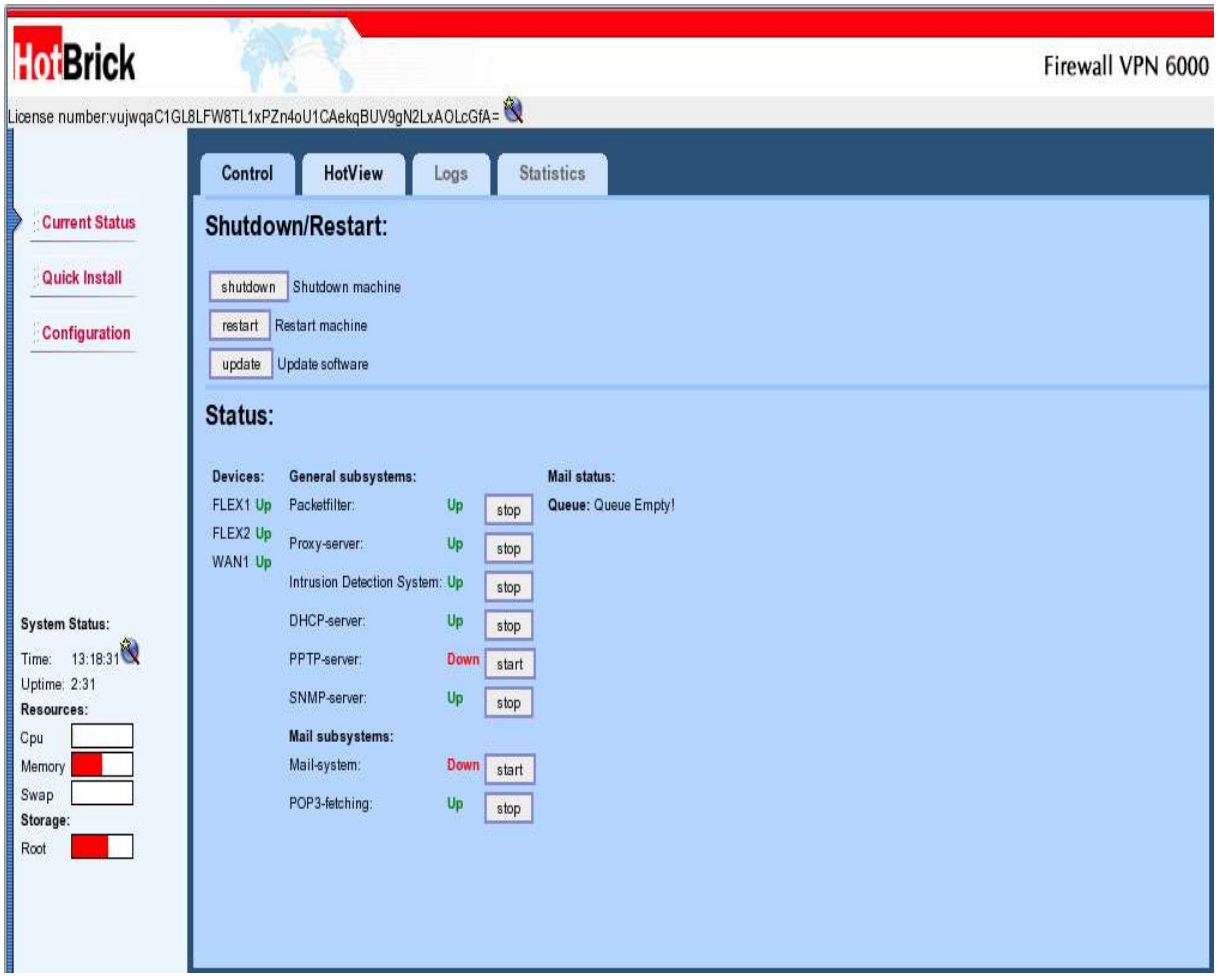
If you wish to keep your existing DHCP server active, we must deactivate the HotBrick VPN 6000's built-in DHCP server before connecting the firewall to your local network.

If you need to disable the HotBrick VPN 6000's built-in DHCP server:

➔ Click on the red text “Current Status” on the left hand side of the screen to enter the “Current Status” context.

➔ Activate the “Control” tab by clicking it once.

➔ In the “Control” page, in the “Subsystems” table, find the line that says “DHCP Server” and click on the corresponding “Stop” button.



1.11 Connecting LAN and WAN cables

Now that we have everything set up correctly, we can perform the final step in the hardware installation of the HotBrick VPN 6000. The firewall is now fully ready to be deployed.

- ➔ Power down the firewall (using the power switch on the back of the device).
- ➔ Power down your notebook or laptop.
- ➔ Detach the network cables from the PC or notebook and the firewall.
- ➔ Using one of the bundled RJ45 UTP cables, connect the WAN1 interface to the router or modem used for your primary (default) Internet connection.
- ➔ If you make use of a secondary (fall back) Internet connection, connect the WAN2 interface to the modem or router used for your secondary (fall back) Internet connection.
- ➔ Using one of the bundled RJ45 UTP cables, connect the FLEX1 interface on the firewall to the switch, router or hub you will use for your local network.
- ➔ Power up the firewall (using the power switch on the back of the device).
- ➔ Check for three beeps to indicate the device has booted up correctly. If you do not hear the three beeps, please refer to section 1.12 (Errors and recovery).
- ➔ Check that WAN1, WAN2 (if in use) and FLEX1 connection LED's (above the corresponding network ports) light up. If one does not, please refer to section 1.12 (Errors and recovery).

1.12 Errors and recovery

Symptom: Check/Solution:

I did not hear three beeps.

Check power cable and insure wall socket has power. Power off the device. Wait 30 seconds. Switch the device on again. If the device fails to beep again the hardware may be at fault. Contact your sales representative for support.

The FLEX1 connection LED doesn't light up when I connect my notebook/PC

Check the cable connection. Make sure you use the network cables bundled with your HotBrick VPN 6000. Verify that both your PC/notebook and your firewall have power and are switched on.

I use an operating system other than Windows 2000/Windows XP/Mac OS X. How am I to enable DHCP on my system?

That information falls outside of the scope of this manual. Please contact your system administrator for support.

DHCP configuration of my system yields the wrong IP Address

If the address you obtain starts with 169.254., or if you get no address at all, then the connection between the firewall and your PC/notebook may be at fault. Check the connection LED for the FLEX1 port to insure that the device is properly connected.

If the address you obtain starts with anything BUT 169.254 then you may have connected you PC or notebook (and probably the firewall too) to an existing network. Please connect the notebook/PC directly to the firewall's FLEX1 port.

My license key is incorrect

Please write down the hard disk serial number mentioned in the “Setup License Keys” dialog and contact your sales representative for a valid license key.

I can't connect to the firewall's management interface

Make sure you have entered the correct address. Initially (before running the “Quick Install” wizard) this should be https://192.168.99.99:12000.

After you've run the quick install wizard this should be https://<your_firewall's_ip_address>:12000 (https://192.168.0.1:12000 in our example).

(Where <your_firewall's_ip_address> denotes the new IP address you entered for the firewall).

Make sure your web browser supports HTTPS. If you are unsure about this, upgrade your web browser to the latest stable version.