User Manual

NetBoz Firewall – User Manual
www.netboz.net
info@netboz.net

Table of Contents

NetBoz Firewall – User Manual
www.netboz.net
info@netboz.net

NetBoz User Manual

1 Instalation

NetBoz instalation is as easy as insert the CD, insert a blank (DOS formatted) diskette and power up the PC.

However, before doing so, it is necessary to be sure that the PC is NetBoz-compatible, and the diskette must contain a valid NetBoz licence key.

The complete process is as follows:

1.1 Compatible Hardware

Finding a NetBoz-compatible PC is not a difficult task. The minimun requirements are the following:

1.1.1 CPU and Mother Board

Any 586 type CPU fits (Pentium or better):

Pentium, Pentium Pro, Pentium II, Pentium III, Pentium 4 and its variants (Celeron) and the AMD line (Am5x86, K5, K6, Athlon and Duron).

The mother board must have a PCI bus. Its is desirable that it doesn't have an integrated network card. If it has one and NetBoz is not able to detect it automatically, then it should be necessary to disable it from the BIOS and install an additional PCI network adapter.

1.1.2 Memory

NetBoz works with a minimum RAM of 64 MB, while 128 MB are enough for almost all the applications.

1.1.3 Network Cards

Compatible network cards are:

Card	Known as
DEC/Intel DC21x4x ("Tulip")	de
3Com 3cR990 ("Typhoon")	txp
3Com 3c590, 3c595 ("Vortex")	vx
MII bus	miibus
DEC/Intel 21143	dc
Intel EtherExpress PRO/100B (82557, 82558)	fxp
AMD Am79C97x PCI 10/100 NICs	pcn
RealTek 8129/8139	rl
Adaptec AIC-6915 ("Starfire")	sf
Silicon Integrated Systems SiS 900/SiS 7016	sis
Sundance ST201 (D-Link DFE-550TX)	ste

NetBoz Firewall – User Manual
www.netboz.net
info@netboz.net

Card	Known as
Texas Instruments ThunderLAN	tl
SMC EtherPower II (83c170 "EPIC")	tx
VIA Rhine, Rhine II	vr
Winbond W89C840F	wb
Intel Gigabit Ethernet Card ("Wiseman")	wx
3Com 3c90x ("Boomerang", "Cyclone")	xl
Broadcom BCM570x ("Tigon III")	bge

1.1.4 CD ROM

As CD reader any ATA compatible can be used.

As an example, any of the following models is acceptable:

AMD 756, 766
CMD 646, 648 ATA66, and 649 ATA100
Cypress 82C693
Cyrex 5530
HighPoint HPT366 ATA66, HPT370 ATA100, HPT372 ATA133
Intel PIIX, PIIX3, PIIX4
Intel ICH ATA66, ICH2 ATA100, ICH3 ATA100
Promise ATA100 OEM chip (pdc20265)
Promise Fasttrak-33, -66, -100 TX2/TX4
Promise Ultra-33, -66, -100
ServerWorks ROSB4 ATA33
SiS 530, 540, 620
SiS 630, 633, 635, 730, 733, 735
SiS 5591
VIA 82C586 ATA33, 82C596 ATA66, 82C686a ATA66, 82C686b ATA100

NetBoz Firewall – User Manual
www.netboz.net
info@netboz.net

1.2 BIOS Tuning

Before trying to boot from the NetBoz CD, the PC must be prepared to fit the NetBoz operating system (FreeBSD).

Some adjustments may be necessary:

1.2.1 Boot Device

Since NetBoz will boot from the CDROM, the BIOS must be prepared to do so.

Select CD-ROM as the Primary Boot Device.

1.2.2 Plug and Play

The NetBoz operating system **IS NOT** Plug and Play, therefore it is necesary to disable such option in the BIOS.

If you don't do it, NetBoz may be unable to recognize the network adapters.

1.2.3 Shadow Memory

All shadow memory kinds must be disabled.

It is also useful to asign a minimum amount of RAM to the VGA adapter (if it shares RAM with the system).

1.3 Setup

Once passing the prior steps, your PC is ready to become a very powerfull firewall.

> **Warning**: Your PC must have two (2) or three (3) network adapters. NetBoz **will not work** if two or three network adapters are not detected.

1.3.1 Diskette setting

If the NetBoz diskette was not delivered by NetBoz, prepare it as follows:

1. Format it using any version of Windows.
2. Copy the NetBoz licence key on it ("netboz.key" file).
3. Verify that the filename is in lowercase.
4. Verify that the diskette **IS NOT** write-protected.

Once prepared, insert the diskette in the diskette drive, insert the NetBoz CD in the CD-ROM drive and power-up the PC.

1.3.2 Network interface organization

In most of the cases the network cards are recognized in the PCI slot order. In a tower kind PC:

- The upper card (the most close to the processor) is the **WAN** interface.
- The following to the bottom is the **LAN** interface.
- If exists, the card at the bottom is the **DMZ** interface.

NetBoz Firewall – User Manual
www.netboz.net
info@netboz.net

If you want to install more than three network cards, then the web administration interface will not be useful. You must configure and setup NetBoz using directly the configuration files (see section "For Experts").

1.3.3 Administration PC readiness

To configure NetBoz through its web interface, it is necessary to have an administration computer. Such computer can be any Windows 98, 2000, Me or XP PC.

Initially, the administration PC must be configured as DHCP client. To do so, in the Netwok control panel, select "Get an IP automatically" under the TCP/IP protocol.
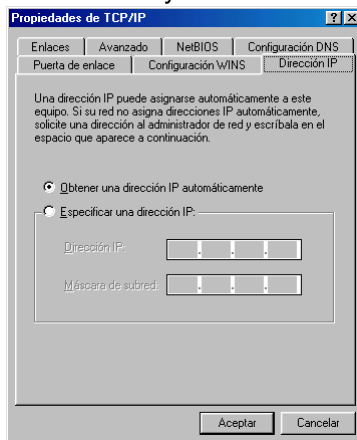
Delete all the Gateways, as well as all the DNS servers.

The administration PC must be connected to the LAN. By default, the LAN will have the DHCP server active.

The connection can be established through a crossing cable or a hub.

1.3.4 LAN I/F detection

By default, NetBoz have the web (https) and ssh administration interfaces enabled at all its network adapters.

The IP numbering assigned by default is the following:

I/F	IP	Network/Mask
WAN	10.0.0.1	10.0.0.0 / 24
LAN	192.168.0.1	192.168.0.0 / 24
DMZ	176.16.0.1	176.16.0.0 / 24

By default, the LAN interface will have its DHCP server enabled. This allows you to connect the administration PC to this I/F and begin a web session using any standard browser (Internet Explorer or Netscape Communicator, for instance).

If the LAN I/F is working fine, it will assign an IP in the range 192.168.0.0/24 to the administration PC. This can be verified using the winipcfg utility (Start menu > execute > winipcfg).

If this procedure fails, then it could be necessary to test the other interfaces to find out wich one was set as the LAN.

NetBoz Firewall – User Manual
www.netboz.net
info@netboz.net
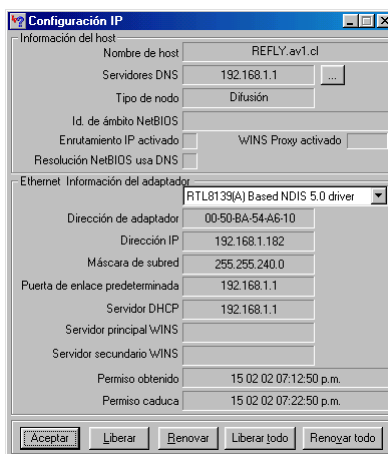
At this point is advisable to maintain NetBoz disconnected from other networks until all the network parameters are correctly assigned through the administration PC.

1.3.5 NetBoz access

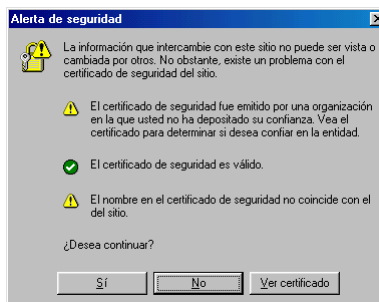The NetBoz web administration I/F is open through the port 45200.

Therefore, the web administration I/F is available at:

WAN	https://10.0.0.1:45200/
LAN	https://192.168.0.1:45200/
DMZ	https://176.16.0.1:45200/

If you have followed the instalation instruction to this point, then you could access the web administration I/F at the URL https://192.168.0.1:45200/.
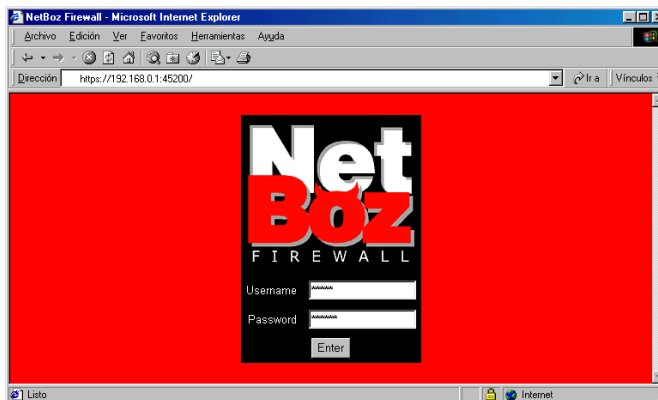
> **Warning**: The protocol must be **https**.

When you attemp to connect the first time, the browser will spot a warning, since the certificate used by NetBoz was not emitted by a recognized entity.

To access de web adminstration interface, you must click on "Yes".

NetBoz Firewall – User Manual
www.netboz.net
info@netboz.net

The NetBoz initial page is the following:

The username is always **admin** (it couldn't be changed).

The default password is **netboz**.

1.3.6 Network configuration

Once inside the administrator, the first thing to do is setup the appropiate values for the networks in wich NetBoz will be connected.
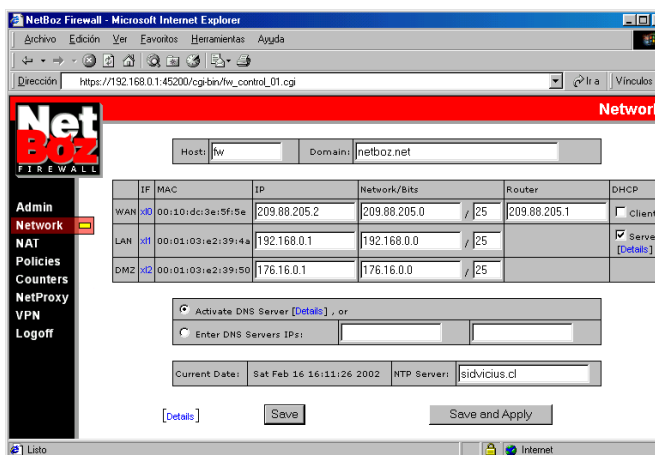
To do so, select the text boxes and insert the values inside each one. They are:

Host	Name of the computer acting as firewall (for example, "netboz")
Domain	Domain in wich the firewall will be inserted.
IP	IP address asigned to the WAN, LAN or DMZ I/F. For the WAN I/F, if DHCP client is checked, then its IP will be assigned by the ISP.

NetBoz Firewall – User Manual
www.netboz.net
info@netboz.net

Network/Bits	Network at wich the WAN, LAN or DMZ is plugged.
	For the WAN I/F, if DHCP client is checked, then its Network and bits will be assigned by the ISP.
	The mask must be entered in bits notation, for example, 192.168.0.0/24 is equivalent to 192.168.0.0/255.255.255.0
Router	For WAN interface only. It is the gateway (router) IP for this network. For the WAN I/F, if DHCP client is checked, then its Router will be assigned by the ISP.
DHCP	The DHCP option is available for the WAN I/F to be a DHCP client and for the LAN I/F to act as a DHCP server.
Activate DNS Server	Through these radio buttons you can choose to use NetBoz as a DNS server or use external DNS servers.
	In case of using external ones, you can enter the IP address of up to two of them.
NTP Server	IP address or name of the NTP server to use.

The "Save" button saves the changes without applying them.

The "Save and Apply" buttom saves and apply the changes immediately.

The first time you configure NetBoz you must apply the changes, since these values will be used by the other features of the system.

> **Warning**: If you modify the LAN values, you can lost contact with NetBoz. In such a case you must adjust the administration PC setting in order to continue the web administration.

The NetBoz web administration was simplified to allow an easy firewall setup, however, if you need more complex settings, the related configuration files are always available through the "Details" links. More information in the "For Experts" section at the end of this manual.

Once the network configuration has been established, you are able to operate NetBoz in a normal way.

The administration web pages available are described in the following sections.

> **Warning**: If you alter the number of network I/Fs on your NetBoz, for example, by removing one interface, then you must start the configuration process all over again, deleting from the diskette all the files except netboz.key.

NetBoz Firewall – User Manual
www.netboz.net
info@netboz.net

2 NetBoz Configuration

2.1 Admin - General Administration
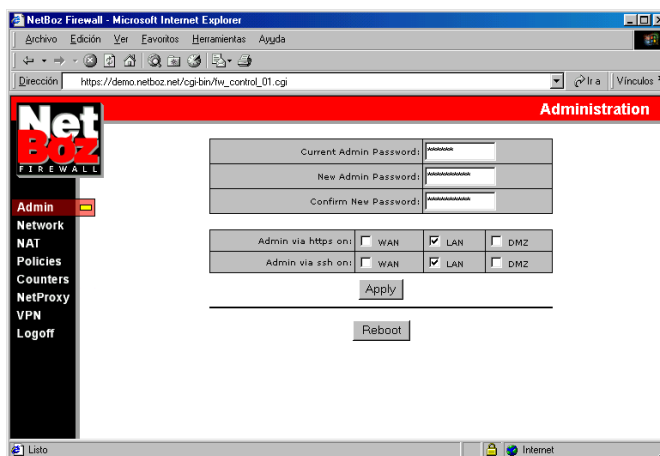
In this page you can change the administrator password and choose the interfaces at which the web and ssh administration should be available.

> **Warning**: Don't forget to change the administration password once NetBoz is installed at the first time. Anyone reading this manual could access your firewall if you don't do so.

2.2 Network – Network Configuration

Refer to point 1.3.6.

2.3 NAT – Services Publishing

Using NetBoz you can publish on the WAN (i.e. Internet) services running on computers instaled inside the DMZ or the LAN networks.

To do this, simply type in the IP and port numbers you wish to use on the WAN and the corresponding IP and port numbers at the internal network (DMZ or LAN).

Then, choose the protocol (TCP or UDP).

To modify a NAT setting, it is necessary to delete and re-enter it. All the settings checked under the title "Delete" will be deleted when you press the "Save" or the "Save and Apply" button.

The "Save" button saves the changes without applying them, allowing to enter all the desired mappings before making them active.

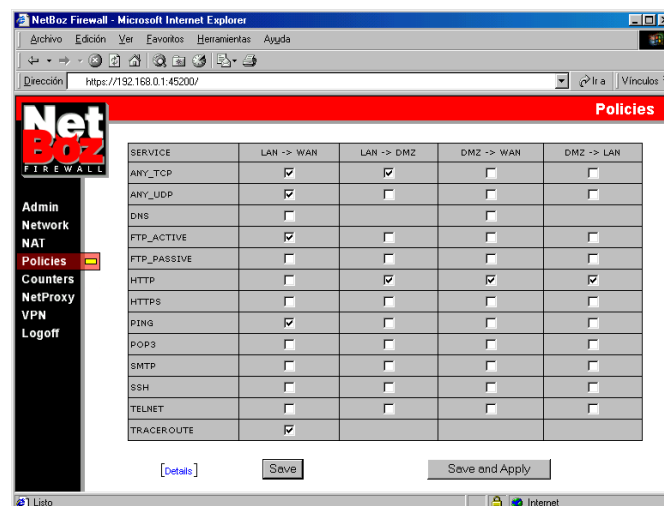The "Save and Apply" button saves and applies any change immediately.

Through the "Details" link it is possible to edit the natd.cfg file directly. See more information in the "For Experts" section.

NetBoz Firewall – User Manual
www.netboz.net
info@netboz.net
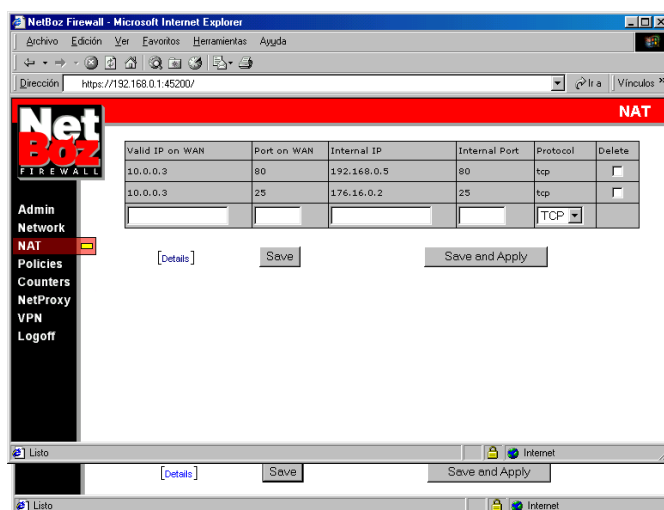
2.4   Policies – Security Policy

The Security Policy is the set of rules applied to the network traffic.

NetBoz performs this duty in a extremely simple way: all the services are presented on a table, in wich each one can be enabled or disabled through checkboxes.

NetBoz makes the translation of these settings to the "true" firewall: FreeBSD ipfw.

The "Save" button saves the changes without applying them.

The "Save and Apply" button saves and applies any change immediately.

The applied rules are visible, and can be edited, directly in the ipfw configuration file (fw.cfg), through the "Details" link. See more information in the "For Experts" section.

NetBoz Firewall – User Manual
www.netboz.net
info@netboz.net

2.5   Counters – Traffic Counters
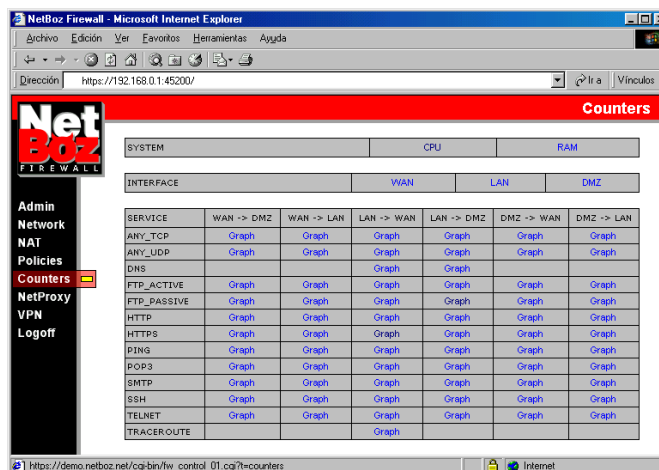
NetBoz delivers graphics information about CPU and RAM usage (useful to find out if an upgrade is necessary), as well as network traffic per interface and per rule.

To see one of these graphics, click on the correspondant link in the Counters page.
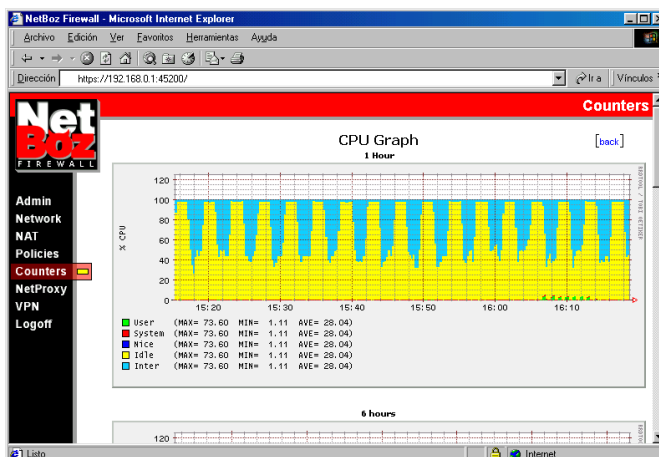
NetBoz builds 1 hour, 6 hours, 1 day, 1 week and 1 month graphs, allowing you to see the variable behaviour over the time.

2.6   NetProxy – Transparent Proxy

This option is available only in NetProxy-enabled NetBozes.

2.7   VPN – Virtual Private Network

This option is available only in VPN-enabled NetBozes

NetBoz Firewall – User Manual
www.netboz.net
info@netboz.net

2.8   Logoff – End of Session

Click on this button to end your session. This avoids others to enter to NetBoz while you're not at your desk.

2.9   Configuration Protection

The NetBoz complete configuration is stored on the diskette, therefore, to protect your settings against any intrusion, eject the diskette, write-protect it and insert it again.

NetBoz doesn't make any writing to the diskette unless you make a configuration change through the web administration, so it will not generate any performance problem.

> **Warning**: If you make any configuration change, wait several minutes before eject the diskette, since the operating system can delay the writing process usinq the internal RAM buffers.

NetBoz Firewall – User Manual
www.netboz.net
info@netboz.net

3   For Experts

NetBoz is merely a FreeBSD server configured to boot from a CD and provided with a web administration interface.

All the NetBoz variable information (configuration files) is stored in the diskette to be used by the FreeBSD standard services.

Therefore, anyone who master these services can configure NetBoz to perform almost any task, eventually without using the supplied web interface.

A brief description of each service is given here.

3.1   net.cfg - NetBoz Settings

In this file the network user preferences are stored. Basically contains the Network page configuration and is the only propietary format file.

The variables are the following:

Variable	Possible Values	Meaning
DMZ_IF	ex: xl2	DMZ interface card identifier
DMZ_IP_0	ex: 176.16.0.1	DMZ IP number
DMZ_MAC	ex: 00:01:03:e2:39:50	DMZ MAC number
DMZ_MSK	ex: 24	DMZ mask (in bits)
DMZ_NET	ex: 176.16.0.0	DMZ network
DNS_1	ex: 192.245.60.2	First DNS server IP
DNS_2	ex: 209.88.205.65	Second DNS server IP
DNS_ON	yes | no	Defines if NetBoz will act or no as DNS server
DOMAIN	ex: netboz.net	NetBoz domain (WAN side)
HOST	ex: fw	NetBoz host name
LAN_DHCP	yes | no	Defines if NetBoz will run or not a DHCP server on the LAN interface
LAN_IF	ex: xl1	LAN interface card identifier
LAN_IP_0	ex: 192.168.0.1	LAN IP number
LAN_MAC	ex: 00:01:03:e2:39:4a	LAN MAC number
LAN_MSK	ex: 24	LAN mask (in bits)
LAN_NET	ex: 192.168.0.0	LAN network
NTP	ex: ntp.uchile.cl	NTP server used to synchronize the PC clock
WAN_DHCP	yes | no	Defines if NetBoz will run or not a DHCP client on the WAN interface
WAN_IF	ex: xl0	WAN interface card identifier
WAN_IP_0	ex: 10.0.0.2	WAN main IP number
WAN_IP_1	ex: 10.0.0.3	WAN secondary IP number (may be many)
WAN_MAC	ex: 00:10:dc:3e:5f:5e	WAN MAC number

NetBoz Firewall – User Manual
www.netboz.net
info@netboz.net

Variable	Possible Values	Meaning
WAN_MSK	ex: 24	WAN mask (in bits)
WAN_NET	ex: 10.0.0.0	WAN network
WAN_ROUTER	ex: 10.0.0.1	WAN gateway (router) IP

3.2   fw.cfg - ipfw configuration

This file corresponds to the FreeBSD ipfw configuration file, where sustitution variables have been used to refer to networks and interfaces:

These variables have the same names usad in the net.cfg file (described above), plus the HPORTS variable, used to refer to the 1024-65535 ports range.

The rules managed by the web administration interface are delimited by comments like:

```
#admin_section
#/admin_section
```

An advanced user can add its own rules outside these comments.

Detailed information about ipfw can be found in the FreeBSD web site (www.freebsd.org).

3.3   policies.proto – Additional Rules

Another way to add custom rules to NetBoz is creating a policies prototipe file in the diskette.

This file must have the name "policies.proto" and contain prototipe rules in the NetBoz Format:

```
<Rulename OriginIF_DestinationIF>
ipfw Rules
...
</ Rulename OriginIF_DestinationIF>
```

for example:

```
<DNS DMZ_WAN>
FWCMD add 24022 allow udp from DMZ_NET HPORTS to ANY 53 in via DMZ_IF
FWCMD add 24022 allow udp from DMZ_NET HPORTS to ANY 53 out via WAN_IF
FWCMD add 24022 allow udp from WAN_IP_0 HPORTS to ANY 53 out via WAN_IF
FWCMD add 24022 allow udp from ANY 53 to DMZ_NET HPORTS in via WAN_IF
FWCMD add 24022 allow udp from ANY 53 to DMZ_NET HPORTS out via DMZ_IF
</DNS DMZ_WAN>
```

The advantage is that such rules will appear inside the Policies page in the web administration interface, therefore it can be easily activated or disabled.

NetBoz Firewall – User Manual
www.netboz.net
info@netboz.net

3.4   natd.cfg – NAT service configuration

This file corresponds exactly to the FreeBSD NAT service configuration (natd).

An advanced user could, for example, map IP ranges or port ranges.

Detailed information about natd can be found in the FreeBSD web site (www.freebsd.org).

3.5   dhcpd.cfg – DHCP server configuration

This file corresponds exactly to the FreeBSD DHCP server configuration (dhcpd).

An advanced user could, for example, define static ranges of IP numbers inside the LAN network, for service setup or for apply special policies to sets of users.

Detailed information about dhcp can be found in the FreeBSD web site (www.freebsd.org).

3.6   named.cfg - Name server configuration

This file corresponds exactly to the FreeBSD DNS server configuration (named).

An advanced user could use NetBoz as a primary DNS, using the diskette to store the zone files of the resolved domains.

Detailed information about named can be found in the FreeBSD web site (www.freebsd.org).

3.7   SSH Administration

The SSH administration interface allows you to log in remotely, like any other Unix server.

SSH gives you a high level of control over NetBoz, since you can check directories, services, edit and copy files, etc., and reboot to aply your changes.

> **Warning**: The SSH prompt can take several minutes in appear. This is normal due to the security checkings NetBoz perform before allow the connection with the client.

As a SSH client, you can use SecureCRT (www.vandyke.com).

NetBoz Firewall – User Manual
www.netboz.net
info@netboz.net

4   Common Problems

Following, some common problems, their causes and solutions:

• **NetBoz does not boot**

- • Verify that the CD-ROM is configured as the boot device in the BIOS.
- • Verify that the diskette is inserted, in good shape and with the netboz.key file wrote in it.
- • Verify that your PC has at least two network interfaces. NetBoz will not boot if you have only one of them.

• **The network adapters are not recognized**

- • Verify that the plug and play is disabled in the BIOS.
- • Verify that the models you are using are in the hardware compatibility list.

• **I forget my password**

- • Dont panic. Delete the "pass" file in the diskette and reboot. Log in with the default password and change it again in the Admin page.