Manual del Usuario

Índice

Manual del Usuario NetBoz

1 Instalación

La instalación de NetBoz es tan fácil como insertar el CD, insertar el diskette y energizar el computador que servirá de firewall.

Sin embargo, antes de hacer esto hay que asegurarse que el PC sea compatible con NetBoz y debe copiarse al diskette la licencia de software (archivo netboz.key).

A continuación se describe el proceso paso a paso.

1.1 Hardware Compatible

Encontrar un computador compatible con NetBoz no es difícil. Los requisitos mínimos son los siguientes:

1.1.1 CPU y Tarjeta Madre

Como procesador, sirve cualquiera del tipo 586 (Pentium o superior):

Pentium, Pentium Pro, Pentium II, Pentium III, Pentium 4 y sus variantes (Celeron) y los AMD Am5x86, K5, K6, Athlon y Duron.

La tarjeta madre debe contar con bus PCI (hace años que todas lo traen). Es preferible que no tenga una tarjeta de red integrada. Si tiene una y NetBoz no la detecta, entonces hay que desactivarla mediante el BIOS y usar sólo tarjetas de red PCI.

1.1.2 Memoria

NetBoz funciona con un mínimo de 64 MB de memoria RAM, siendo 128 MB suficientes para la mayoría de las aplicaciones.

1.1.3 Tarjetas de Red

Las tarjetas de red compatibles son:

Tarjeta	**Reconocida como**
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

Tarjeta	Reconocida como
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

Como lector de CD puede utilizarse cualquier ATA compatible.
En particular, los siguientes modelos son soportados:

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

1.2 Ajustes en el BIOS

Antes de intentar bootear con el CD de NetBoz, debe prepararse el PC para que soporte el sistema operativo de NetBoz (FreeBSD).

Los ajustes necesarios son los siguientes:

1.2.1 Dispositivo de Boot

Ya que se booteará desde el CDROM, debe ajustarse el BIOS para que al menos en primera instancia busque el sector de inicio en este dispositivo. Generalmente esto se conoce como "Primary Boot Device".

1.2.2 Plug and Play

El sistema operativo de NetBoz **NO** es Plug and Play, así que debe deshabilitarse esta opción del BIOS. Si no se hace esto, NetBoz podría no encontrar y por lo tanto no inicializar las tarjetas de red.

1.2.3 Memoria Shadow

Deben deshabilitarse todas las formas de memoria shadow del BIOS y otras.

También es útil asignar el mínimo de memoria posible a la VGA (si es que ésta comparte RAM con el sistema).

1.3 Puesta en Marcha

Una vez chequeados los puntos anteriores, el PC estará listo para transformarse en un poderoso firewall.

> **Importante**: Verifique que dispone de dos o tres tarjetas de red. NetBoz **no funciona** si no detecta dos o más tarjetas de red.

1.3.1 Preparación del Diskette

Si el diskette no ha sido suministrado por NetBoz, prepárelo de la siguiente manera:

1. Formatee un diskette utilizando cualquier versión de Windows.
2. Copie en él la licencia NetBoz (archivo "netboz.key").
3. Verifique que el nombre del archivo quede escrito con letras minúsculas.

Una vez preparado el diskette, introdúzcalo en la disketera, inserte el CD NetBoz y energice el PC. En esta etapa, el diskette **no** debe estar protegido contra escritura.

1.3.2 Organización de las I/F de Red

Generalmente las tarjetas de red son reconocidas en el orden en que se encuentran insertas. En un PC de formato Tower:

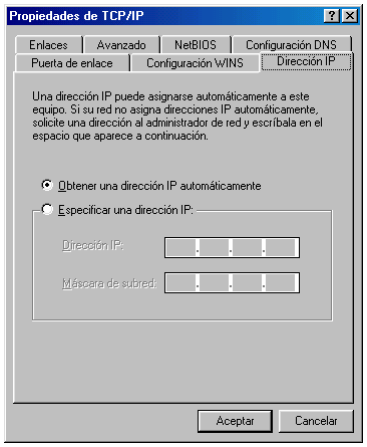
- La de más arriba (más cerca de la CPU) es la interfaz **WAN**.
- La siguiente hacia abajo es la interfaz **LAN**.
- Si existe, la de más abajo es la interfaz **DMZ**.

Si hay más de tres tarjetas de red, entonces la interfaz de administración web no será útil. Sólo podrá configurarse NetBoz y establecerse políticas manipulando directamente los archivos de configuración (ver sección "Para Expertos").

1.3.3 Preparación del PC de Administración

Para configurar NetBoz a través de su interfaz web es necesario contar con un PC de Administración, el cual puede ser un computador PC con Windows 98, 2000 o XP.

Este computador debe ser configurado como cliente DHCP, para lo cual basta con indicar en las "propiedades" del protocolo TCP/IP "Obtener una dirección IP automáticamente".



En "Puerta de Enlace" deben eliminarse todas, al igual que los servidores DNS.

El PC de administración debe conectarse a la interfaz LAN, la cual cuenta por defecto con su servidor DHCP activo.

La conexión puede ser directa mediante de un cable cruzado, o bien conectando ambos equipos a un hub.

1.3.4 Detección de la I/F LAN

Por defecto, NetBoz posee habilitada la administración web (https) y ssh en todas las interfaces.

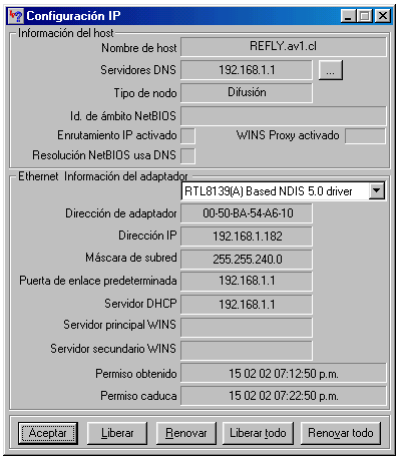
Las numeraciones IP asignadas por defecto a cada una de ellas son las siguientes:

Interfaz	IP	Red y Máscara
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

Por defecto también la interfaz LAN posee el servicio DHCP habilitado. Esto permite conectar el PC de administración a esta interfaz y comenzar la sesión web utilizando un browser estándar (Internet Explorer o Netscape communicator).

Si la interfaz está operando correctamente, asignará un número IP en el rango 192.168.0.0/24 al PC. Esto puede ser verificado utilizando el utilitario winipcfg (Menú inicio > ejecutar > winipcfg).

Si esto no ocurriera, entonces hay que probar las otras interfaces para así detectar cuál de ellas fue asignada como LAN.



En una primera instancia es conveniente no conectar NetBoz a ninguna otra red hasta asignar los parámetros de red definitivos a través del PC de administración.

1.3.5 Ingreso a NetBoz

La interfaz de administración web es accesible a través del puerto 45200.

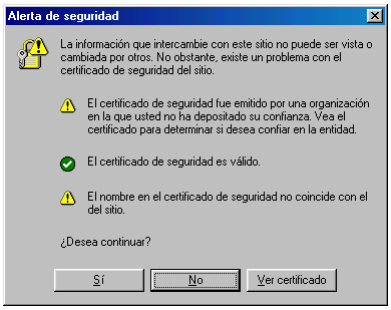
De esta manera, por defecto la interfaz de administración se encuentra disponible en:

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

Si Ud. ha seguido las instrucciones hasta aquí, entonces podrá acceder a la interfaz de administración web en la dirección https://192.168.0.1:45200/.

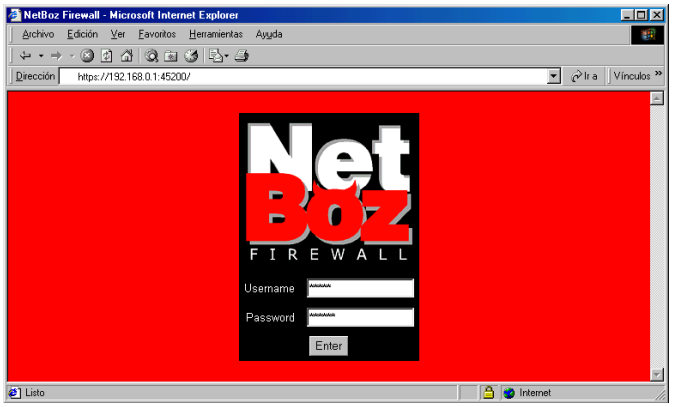
Importante: El protocolo es **https**.

Al conectarse por primera vez, el browser pondrá una advertencia, dado que el certificado utilizado para establecer la comunicación SSL no ha sido emitido por una entidad reconocida.



Para acceder a NetBoz debe hacerce click en el botón "Si".

La página web de ingreso es la siguiente:

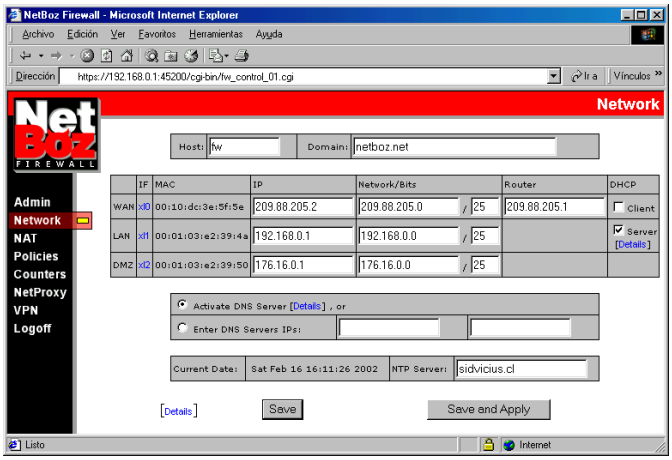


El nombre de usuario es siempre **admin** (no se puede cambiar).

La contraseña por defecto es **netboz**.

1.3.6 Configuración de la Red

Una vez dentro del administrador, lo primero que debe hacerse es establecer los valores definitivos para las redes a las que se conectará NetBoz.



Seleccione las opciones de interés e ingrese los datos en los casilleros correspondientes. Estos son:

Host	Nombre del computador que servirá de firewall (por ejemplo, "netboz")
Domain	Dominio en que estará inserto el firewall.
IP	Dirección IP asignada a la interfaz WAN. LAN o DMZ, según sea el caso. Para la interfaz WAN, si se usa cliente DHCP, este número será asignado por el ISP correspondiente.

Network/Bits	Identificación de la red a la que está conectada la WAN, la LAN o la DMZ, según sea el caso. Para la interfaz WAN, si se usa cliente DHCP, este valor será asignado por el ISP correspondiente. La máscara debe indicarse en la notación de número de bits, por ejemplo: 192.168.0.0/24, lo que es equivalente a 192.168.0.0/255.255.255.0
Router	Sólo para la interfaz WAN, es la dirección IP del router de salida (Gateway) de esta red.
DHCP	La opción DHCP está disponible para que la interfaz WAN sea cliente DHCP y para que la interfaz LAN actúe como servidor DHCP.
Activate DNS Server	A través de estos radio buttons, Ud. puede escoger entre usar su NetBoz como servidor DNS o utilizar servidores de nombres externos. En caso de usar servidores externos, puede ingresar las direcciones IP de hasta dos de ellos.
NTP Server	Dirección IP o nombre del servidor NTP que se utilizará.

El botón "Save" permite guardar los cambios sin aplicarlos.

El botón "Save and Apply" guarda y aplica los cambios de inmediato.

La primera vez que Ud. configure su NetBoz debe escoger el botón "Save and Apply", ya que los datos que ingrese serán utilizados por el resto del sistema.

> **Importante**: Si Ud. modifica los valores de la interfaz LAN, perderá contacto con NetBoz, debiendo ajustar su PC para poder continuar administrandolo vía web.

La interfaz de administración web de NetBoz ha sido simplificada para facilitar al máximo la puesta en marcha de su firewall, sin embargo, si Ud. requiere de seteos más complejos, los archivos de configuración correspondientes estarán siempre al alcance a través de los links "Details". Más información en la sección "Para Expertos" de este manual.

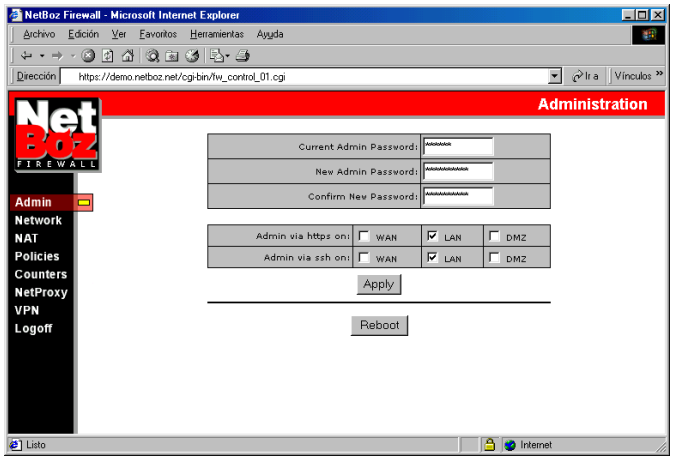
Una vez establecida la configuración de red, Ud. está en condiciones de operar su NetBoz en forma normal.

A continuación se describen las páginas de administración disponibles.

> **Importante**: Si Ud. modifica la cantidad de interfaces de NetBoz, entonces debe borrar todos los archivos del diskette (a excepción de la licencia) y comenzar nuevamente toda la instalación.

2 Configuración de NetBoz

2.1 Admin - Administración General



En esta página se puede cambiar la contraseña del administrador y escoger a través de qué interfaces podrá administrarse NetBoz.

> **Importante**: Al instalar NetBoz por primera vez, no olvide cambiar la contraseña, ya que de otra manera cualquiera que lea este documento estará en condiciones de tomar el control de su red.

2.2 Network - Configuración de la Red

Descrita en punto 1.3.6.

2.3 NAT - Publicación de Servicios

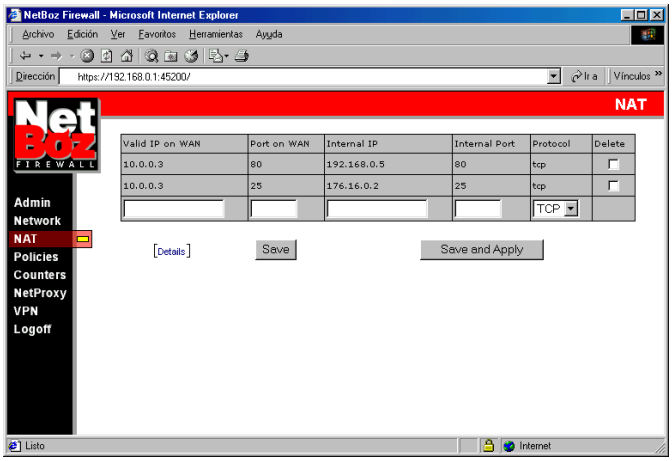
Usando NetBoz Ud. puede hacer visibles en la WAN (o sea, en Internet) servicios prestados por computadores instalados en la DMZ o en la LAN.

Para ello simplemente inserte el número IP y la puerta por la que desea que se acceda en la WAN (Valid IP on WAN, Port on WAN) y el número IP y la puerta del servicio en el computador instalado en la DMZ o la LAN (Internal IP, Internal Port).

El protocolo a mapear puede ser TCP o UDP (Protocol).

Para modificar un mapeo NAT, es necesario borrarlo e ingresarlo nuevamente. Todos los mapeos marcados con el checkbox bajo el rótulo "Delete" serán eliminados al hacer click sobre el botón "Save" o el botón "Save and Apply".

El botón "Save" guarda los cambios sin aplicarlos, lo cual permite ingresar todos los mapeos NAT deseados antes de hacerlos efectivos.



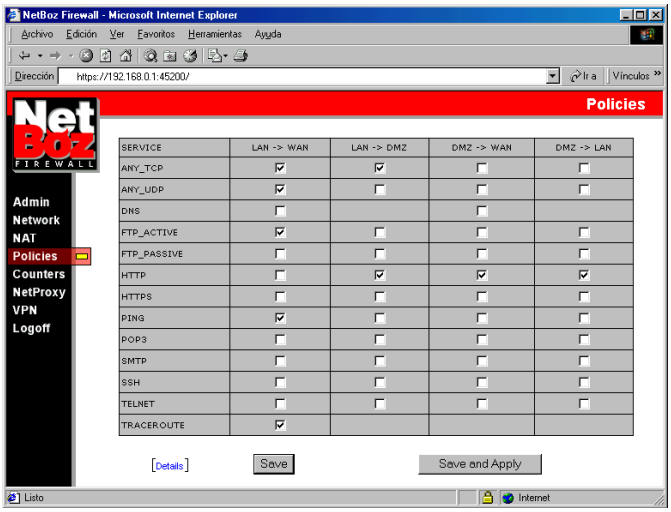
El botón "Save and Apply" guarda y aplica los cambios de inmediato.

A través del link "Details" es posible editar el archivo natd.cfg directamente. Más información en la sección "Para Expertos".

2.4 Policies - Política de Seguridad

La Política de Seguridad corresponde al conjunto de reglas aplicadas al tráfico de sus redes.

En NetBoz esto se hace con extrema facilidad: basta con habilitar los servicios requeridos desde una interfaz a otra.



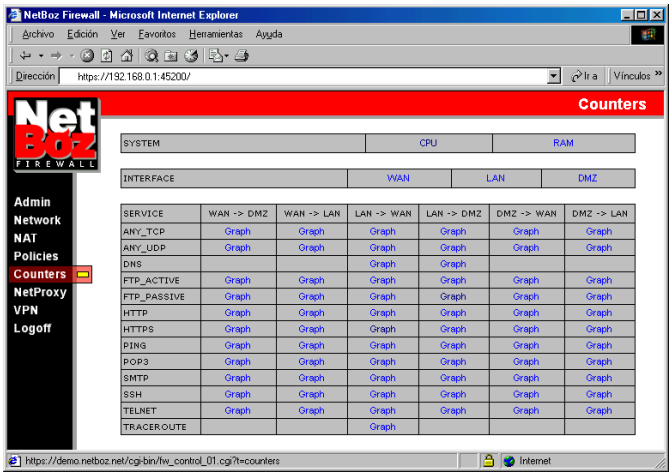
NetBoz se encarga de traducir estas preferencias en una serie de reglas para el "verdadero" firewall: ipfw, de FreeBSD.

El botón "Save" permite guardar los cambios sin aplicarlos.

El botón "Save and Apply" guarda y aplica los cambios de inmediato.

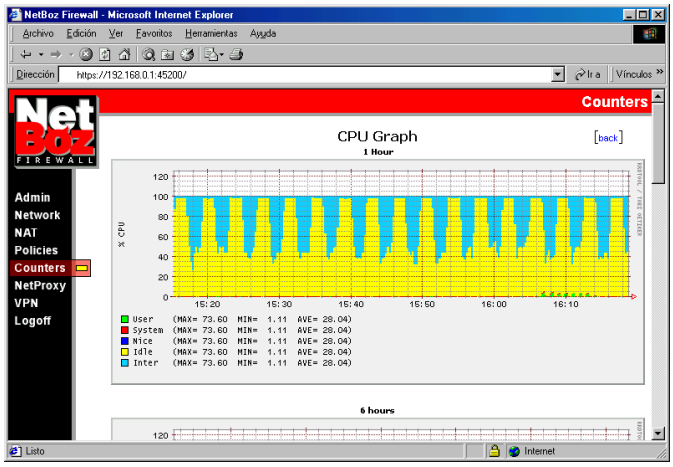
Las reglas aplicadas son visibles, y pueden ser editadas, directamente en el archivo de configuración fw.cfg a través del link "Details". Más información en la sección "Para Expertos".

2.5 Counters - Gráficos de Tráfico



NetBoz entrega información gráfica sobre el uso de la CPU y la RAM del PC (muy útil para decidir si hace falta mejorar el hardware), y de tráfico por interfaz y por regla.

Para ver un gráfico, basta hacer click en el link correspondiente.



NetBoz entrega gráficos con escalas de 1 hora, 6 horas, 1 día, 1 semana y un mes, lo cual permite apreciar la evolución de la variable en el tiempo.

2.6 NetProxy - Protección para IIS

Esta opción está activa sólo en NetBoz habilitados.

2.7 VPN - Redes Privadas Virtuales

Esta opción está activa sólo en NetBoz habilitados.

2.8 Logoff - Fin de sesión

Para terminar su sesión de administración, haga click en este botón del menú.

2.9 Protección de la Configuración

La configuración completa de NetBoz es almacenada en el diskette, por lo tanto, para proteger la configuración de NetBoz contra cualquier intrusión, basta retirar el diskette, protegerlo contra escritura y luego insertarlo nuevamente.

NetBoz no escribe en el diskette a menos que se trate de un cambio en la configuración realizado a través de la interfaz web, así que esto no generará problemas de funcionamiento.

Importante: Al hacer un cambio de configuración, espere unos minutos antes de retirar el diskette y protegerlo, ya que puede que el sistema operativo retarde el proceso de escritura física al diskette, por tratarse de un dispositivo lento.

3 Para Expertos

NetBoz no es más que un servidor FreeBSD configurado para bootear desde un CDROM y dotado de una interfaz web para administración.

Toda la información variable de NetBoz (configuraciones) es almacenada en el diskette en archivos de configuración que corresponden a los utilizados por los servicios correspondientes en FreeBSD.

De esta manera, cualquiera que domine estos servicios puede configurar NetBoz para que cumpla prácticamente cualquier función, eventualmente prescindiendo de la interfaz web de administración.

Una descripción de los servicios y archivos de configuración utilizados se entrega a continuación.

3.1 net.cfg - Seteos de NetBoz

En este archivo quedan establecidas las preferencias del usuario en cuanto a redes. Básicamente almacena la configuración de la página Network y es el único archivo de formato propietario.

Las variables son las siguientes:

Variable	Valores posibles	Explicación
DMZ_IF	ej: xl2	Identificador de la tarjeta de interfaz DMZ
DMZ_IP_0	ej: 176.16.0.1	Número IP asignado a la interfaz DMZ
DMZ_MAC	ej: 00:01:03:e2:39:50	Identificador MAC de la interfaz DMZ
DMZ_MSK	ej: 24	Máscara, en número de bits, asociada a la red de la interfaz DMZ
DMZ_NET	ej: 176.16.0.0	Red asociada a la red de la interfaz DMZ
DNS_1	ej: 192.245.60.2	Dirección IP del primer servidor de nombres.
DNS_2	ej: 209.88.205.65	Dirección IP del segundo servidor de nombres.
DNS_ON	yes | no	Define si se activa o no NetBoz como servidor de nombres.
DOMAIN	ej: netboz.net	Dominio donde está inserto NetBoz (por el lado de la WAN)
HOST	ej: fw	Nombre que recibe el computador NetBoz.
LAN_DHCP	yes | no	Define si se activa o no el servidor DHCP en la interfaz LAN
LAN_IF	ej: xl1	Identificador de la tarjeta de interfaz LAN
LAN_IP_0	ej: 192.168.0.1	Número IP asignado a la interfaz LAN
LAN_MAC	ej: 00:01:03:e2:39:4a	Identificador MAC de la interfaz LAN
LAN_MSK	ej: 24	Máscara, en número de bits, asociada a la red de la interfaz LAN
LAN_NET	ej: 192.168.0.0	Red asociada a la red de la interfaz LAN
NTP	ej: ntp.uchile.cl	Servidor NTP utilizado para sincronizar el reloj de NetBoz
WAN_DHCP	yes | no	Define si se aplica DHCP cliente a la interfaz WAN.
WAN_IF	ej: xl0	Identificador de la tarjeta de interfaz WAN

Variable	Valores posibles	Explicación
WAN_IP_0	ej: 10.0.0.2	Número IP principal asignado a la interfaz WAN
WAN_IP_1	ej: 10.0.0.3	Número IP asignado a la interfaz WAN
WAN_MAC	ej: 00:10:dc:3e:5f:5e	Identificador MAC de la interfaz WAN
WAN_MSK	ej: 24	Máscara, en número de bits, asociada a la red de la interfaz WAN
WAN_NET	ej: 10.0.0.0	Red asociada a la red de la interfaz WAN
WAN_ROUTER	ej: 10.0.0.1	Número IP del router (Gateway) de la WAN.

3.2 fw.cfg - Configuración de ipfw

Este archivo corresponde a la configuración del servicio de firewall de FreeBSD, ipfw, donde se han utilizado variables de sustitución para referirse a distintas redes e interfaces:

Estas variables corresponden a las utilizadas en el archivo net.cfg, más la variable HPORTS, que se usa para referirse al rango de puertas 1024 - 65535.

Las reglas manejadas por la interfaz web de administración están delimitadas por comentarios del tipo:

```
#admin_section
#/admin_section
```

Un usuario avanzado puede agregar reglas propias fuera de estos marcadores.

Más información puede encontrarse en el sitio web de FreeBSD (www.freebsd.org).

3.3 policies.proto - Reglas Adicionales

Otra forma de agregar reglas es creando un archivo de nombre "policies.proto" en el diskette.

Este archivo debe contener las reglas de acuerdo al formato NetBoz:

```
<NombreRegla IForigen_IFdestino>
Reglas ipfw
...
</NombreRegla IForigen_IFdestino>
```

por ejemplo:

```
<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>
```

Esta modalidad tiene la ventaja de que la regla aparecerá dentro de la página "policies" en la interfaz de administración web, pudiendo por lo tanto activarse o desactivarse mucho más facilmente.

3.4 natd.cfg - Configuración del servicio NAT

Este archivo corresponde exactamente a la configuración del servicio NAT de FreeBSD, natd.

Un usuario avanzado podrá, por ejemplo, mapear rangos de IPs o rangos de puertas por completo.

Más información puede encontrarse en el sitio web de FreeBSD (www.freebsd.org).

3.5 dhcpd.cfg - Configuración del servidor DHCP

Este archivo corresponde exactamente a la configuración del servicio DHCP de FreeBSD, dhcpd.

Un usuario avanzado podrá definir rangos para números ip fijos dentro de la LAN, ya sea para definir servicios o para aplicar a esos usuarios políticas de seguridad especiales.

Más información puede encontrarse en el sitio web de FreeBSD (www.freebsd.org).

3.6 named.cfg - Configuración del servidor de Nombres

Este archivo corresponde exactamente a la configuración del servicio de nombres de FreeBSD, natd.

Un usuario avanzado podrá utilizar NetBoz como servidor DNS primario alterando este archivo y copiando en el diskette los archivos de zona de los dominios que resolverá.

Más información puede encontrarse en el sitio web de FreeBSD (www.freebsd.org).

3.7 Administración vía SSH

La interfaz SSH permite al administrador ingresar remotamente a la máquina, tal como se hace con cualquier servidor UNIX.

De esta manera, el administrador puede revisar directorios, editar los archivos de configuración mediante el editor vi (incluido en NetBoz), copiar archivos y rebootear para aplicar los cambios.

> **Importante**: Puede que el prompt SSH demore unos minutos en aparecer. Esto es normal y se debe a los chequeos de seguridad que realiza NetBoz antes de conectarse con el cliente.

Como cliente SSH se recomienda SecureCRT (www.vandyke.com).

4 Problemas Comunes

A continuación, algunos problemas comunes, sus posibles causas y soluciones.

- **NetBoz no Bootea**
  - Verifique que el CDROM esté configurado como dispositivo de Boot en el BIOS.
  - Verifique que el diskette se encuentre en buen estado y con el archivo de licencia (netboz.key) grabado en él.
  - Verifique que su PC tenga al menos dos interfaces de red.
    NetBoz no funciona si posee una sola.

- **Las Tarjetas de Red no son reconocidas**
  - Verifique que el Plug and Play esté desactivado en el BIOS.
  - Verifique que los fabricantes y modelos se encuentren dentro de la lista de compatibilidad.

- **Olvidé mi Contraseña**
  - No se preocupe. Simplemente borre el archivo "pass" del diskette, resetee NetBoz, ingrese con la contraseña por defecto y luego cámbiela nuevamente en la página Admin.