```
# ======================================================================$
# $Id: ipkungfu.conf 57 2005-11-02 17:04:20Z s0undt3ch $
# ======================================================================$

# Please read the README and FAQ for more information

# Some distros (most notably Redhat) don't have
# everything we need in $PATH so we specify it here.
# Make sure modprobe, iptables, and route are here,
# as well as ordinary items such as echo and grep.
# Default is as shown in the example below.
#PATH=/sbin:/usr/sbin:/bin:/usr/bin:/usr/local/bin:/usr/local/sbin

# Set the path to ipkungfu's runtime error log.
# Default: /var/log/ipkungfu.log
IPKUNGFU_LOG=/var/log/ipconfig.log

# Your external interface
# This is the one that connects to the internet.
# Ipkungfu will detect this if you don't specify.
#EXT_NET="eth0"
#EXT_NET="eth1"
#EXT_NET="ppp0"

# Your internal interfaces, if any.  If you have more
# than 1 internal interface, separate them with
# spaces.  If you only have one interface, put "lo"
# here. Default is auto-detected.
#INT_NET="eth0"
#INT_NET="eth1"
#INT_NET="lo"

# IP Range of your internal network.  Use "127.0.0.1"
# for a standalone machine.  Default is a reasonable
# guess. Separate multiple ranges with spaces.
LOCAL_NET="192.168.0.0/255.255.0.0"

# Set this to 0 for a standalone machine, or 1 for
# a gateway device to share an Internet connection.
# Default is 1.
GATEWAY=1
```

```
# TCP ports you want to allow for incoming traffic
# Don't add ports here that you intend to forward.
# This should be a list of tcp ports that have
# servers listening on them on THIS machine,
# separated by spaces. You can add port ranges
# delimited by hyphens, such as "20-22". Default
# is none.
#ALLOWED_TCP_IN="21 22"

# UDP ports to allow for incoming traffic
# See the comments above for ALLOWED_TCP_IN
#ALLOWED_UDP_IN=""



# Temporarily block future connection attempts from an
# IP that hits these ports (If module is present)
# Hits to these ports will be logged as "BADGUY" hits
# regardless of log.conf settings.
FORBIDDEN_PORTS="135 137 139"

# Drop all ping packets?
# Set to 1 for yes, 0 for no. Default is no.
BLOCK_PINGS=1

# Possible values here are "DROP", "REJECT", or "MIRROR"
#
# "DROP" means your computer will not respond at all. "Stealth mode"
#
# "REJECT" means your computer will respond with a
# message that the packet was rejected.
#
# "MIRROR", if your kernel supports it, will swap the source and
# destination IP addresses, and send the offending packet back
# where it came from.  USE WITH EXTREME CAUTION! Only use this if you$
# understand the consequences.
#
# The safest option, and the default in each case,,  is "DROP". Don't c$
# unless you fully understand this.



# What to do with 'probably malicious' packets
#SUSPECT="REJECT"
```

```
SUSPECT="DROP"

# What to do with obviously invalid traffic
# This is also the action for FORBIDDEN_PORTS
#KNOWN_BAD="REJECT"
KNOWN_BAD="DROP"

# What to do with port scans
#PORT_SCAN="REJECT"
PORT_SCAN="DROP"

# How should ipkungfu determine your IP address? The default
# answer, "NONE", will cause ipkungfu to not use the few
# features that require it to know your external IP address.
# This option is good for dialup users who run ipkungfu on
# bootup, since dialup users rarely use the features that
# require this, and the IP address for a dialup connection
# generally isn't known at bootup.  "AUTO" will cause
# ipkungfu to automatically determine the IP address of
# $EXT_NET when it is started.  If you have a static IP
# address you can simply enter your IP address here.
# If you do port forwarding and your ISP changes your IP
# address, choose NONE here, or your port forwarding
# will break when your IP address changes. Default is
# "NONE".
#GET_IP="NONE"
#GET_IP="AUTO"
#GET_IP="128.238.244.16"

# If the target for identd (113/tcp) is DROP, it can take
# a long time to connect to some IRC servers. Set this to
# 1 to speed up these connections with a negligible cost
# to security.  Identd probes will be rejected with the
# 'reject-with-tcp-reset' option to close the connection
# gracefully. If you want to actually allow ident probes,
# and you're running an identd, and you've allowed port
# 113 in ALLOWED_TCP_IN, set this to 0. Default is 0.
#DONT_DROP_IDENTD=0

# Set this to 0 if you're running ipkungfu on a machine
# inside your LAN.  This will cause private IP addresses
# coming in on $EXT_NET to be identified as a spoof,
```

```
# which would be inaccurate on intra-LAN traffic

# This will cause private IP addresses coming in on
# $EXT_NET to be identified as a spoof. Default is 1.
#DISALLOW_PRIVATE=1

# For reasons unknown to me, ipkungfu sometimes causes
# kernel panics when run at init time. This is my
# attempt to work around that.  Ipkungfu will wait
# the specified number of seconds before starting, to
# let userspace/kernel traffic catch up before executing.
# Default is 0.
#WAIT_SECONDS=5

# This option, if enabled, will cause ipkungfu to set
# the default policy on all builtin chains in the filter
# table to ACCEPT in the event of a failure.  This is
# intended for remote administrators who may be locked
# out of the firewall if ipkungfu fails.  A warning to
# this effect will be echoed so that the situation can be
# rectified quickly.  This is the same as running
# ipkungfu with --failsafe.  Default is 0.
#How should ipkungfu=0

# Configurable list of kernel modules to load at runtime.
# If no list is provided, the default and needed ones,
# ip_nat_irc, ip_conntrack_ftp ip_nat_ftp ip_conntrack_irc,
# will still be loaded.
#MODULES_LIST=""
```