Mon Motha 's IPTables Firewall Configuration Reference Guide

Version 2.3.8

This is a detailed guide of the configuration options within {{https://web.archive.org/web/20041217084425im_/http://www.mplug.org/phpwiki/themes/Hawaiian/images/flower.png?nolink&|http}}MonMotha's IPTables script, a mature and easy to configure Linux 2.4 kernel Netfilter script that will do firewalling, routing, NAT, IP masquerading, and “Cable/DSL router”ing as CompUSA sales people call it.

This is a wiki page. **Please** feel free to comment where you think additional information might be useful to people configuring the script.

Notation Conventions Used

- Standard CIDR notation is always permitted when an IP address is called for. This may be used to specify that a rule shall apply to an entire network rather than a single host.
- Network/Mask notation is also permitted, though CIDR is usually more readable and easier for the “networking gurus” to understand should you need to ask for help
- LOCIP option: See bottom
- When specifying multiple parameters for an option, separate with a space.
- The script currently parses by simply setting IFS and running the fields in order; all fields of an option not specifically specified as optional are required. 0/0 may be used if you wish to specify any host; 0-65535 can be used to specify any port.
    - Don't try to confuse the parser because it's easy to do so. This will be addressed in a future version (and patches welcome!)
- iptables standard start:stop format for port ranges is allowed for some options (not port forwards though), but all options accept start-stop as of 2.3.8-pre7. It is preferred to use start-stop rather than start:stop when specifying a portrange.

Main Configuration Section

IPTABLES=“/usr/local/sbin/iptables”

- Location of the **iptables** tool on your system. Usually **/sbin/iptables** when installed from packages. The default for the source distribution (from {{https://web.archive.org/web/20041217084425im_/http://www.mplug.org/phpwiki/themes/Hawaiian/images/flower.png?nolink&|http}}http://www.netfilter.org) is **/usr/local/sbin/iptables**.

TCP_ALLOW=““

- TCP ports to allow on incoming connections to the firewall itself (localhost) from the Internet. Add only the ports that you need for services like SSHD, Web Servers, FTP servers, etc. Seperate port numbers with spaces like “22 80 443” Keep this as short as possible for security. These also apply to any computers behind the firewall that have public IPs.

UDP_ALLOW="68 6112 6119 4000"

- UDP ports to allow on incoming connections to the firewall itself (localhost). The defaults are what you need to play all battle.net games (including Starcraft and Diablo][) and to act as a DHCP client if the connection tracker fails. These also apply to any computers behind the firewall.

INET_IFACE="eth0"

- Interface device to the Internet. (probably eth1 or eth0 for cable, leased line, and non PPPoE DSL; ppp0 for dialup or PPPoE DSL)
- As of 2.3.8-pre8, multiple interfaces are permitted here

LAN_IFACE="eth1"

- Interface device(s) to your internal LAN. This is probably eth0 or eth1.
- As of 2.3.8-pre5, multiple interfaces are permitted here
- Packets from devices specified as LAN interfaces are completely trusted with regard to what it can access. It has access to all resources available from the firewall box itself (there are no filters outbound from it, only inbound to it). If you desire filtering from a LAN segment to the local firewall box, set it as an INET_IFACE and use LOCIP on your allows, and do not put them in INTERNAL_LAN.

INTERNAL_LAN="192.168.0.0/24 192.168.1.0/24"

- The ENTIRE internal LAN. (If you have multiple subnet's, separate with spaces). This should also set up all you need to use the firewall box as a router between subnets (assuming your routing table is properly configured).
- **/24** means subnet 255.255.255.0, **/8** is 255.0.0.0 (for 10.x.x.x). See CIDR Notation
- The INTERNAL_LAN is completely trusted, see above.

MASQ_LAN="192.168.0.0/24 192.168.1.0/24"

- The internal network(s) to be masqueraded. These IP addresses should be within the three ranges specified by {{https://web.archive.org/web/20041217084425im_/http://www.mplug.org/phpwiki/themes/Hawaiian/images/flower.png?nolink&|http}}RFC 1918 reserved for internal networks.

SNAT_LAN=""

- Internal networks/hosts to use static NAT (format is <internal ip or network>:<external ip>). This is for network address translation of real IP addresses on the Internet side to certain {{https://web.archive.org/web/20041217084425im_/http://www.mplug.org/phpwiki/themes/Hawaiian/images/flower.png?nolink&|http}}RFC 1918 addresses on the internal LAN. This can replace masquerading if you have a static IP and will also allow you to keep connections going if the interface drops momentarily.

DROP="TREJECT"

- What to do with packets we don't want:
  - DROP: Basically ignore the packet, no further action will be taken (good for not allowing

nmap to detect your operating system)
    - REJECT: Respond with an error, then DROP the packet
    - TREJECT: Respond with tcp-reset for TCP or normal REJECT for other protocols, then DROP the packet
    - LDROP: log the packet then DROP it
    - LREJECT: log the packet then REJECT it
    - LTREJECT: log the packet then TREJECT it
- You probably want TREJECT as this will make your firewalled ports show up as if they were not open at all. Use LTREJECT if you want to log it too.

DENY_ALL=""

- Internet hosts to explicitly deny from accessing your system at all. This is an incoming only block (you can still connect to them), and will take the system wide drop policy.

DENY_HOSTWISE_TCP="192.168.1.1>110"

- Specific hosts denied access to specific TCP ports; format is "IP>PORT"

DENY_HOSTWISE_UDP="192.168.1.1>27015"

- Specific hosts denied access to specific UDP ports; format is "IP>PORT"

BLACKHOLE=""

- Hosts you don't want to have anything to do with (this is a bidirectional deny), this can have it's own policy (like DROP) to make your box ignore flooders and other abusers after you've identified them and added them to this.

BLACKHOLE_DROP="DROP"

- What to do with stuff from blackholed hosts. Takes the same options as DROP= above.

ALLOW_HOSTWISE_TCP="123.123.123.123>113"

- Specific hosts allowed access to specific TCP ports; format is "IP>PORT"

ALLOW_HOSTWISE_UDP="123.123.123.123>68"

- Specific hosts allowed access to specific UDP ports; format is "IP>PORT"

TCP_FW=""

- Port forwards on TCP. This allows you to forward one (or a range of ports, use a - between the start and stop ports) port from the external interface on the NAT box to the same or a different port on an internal HOST. This can also be used between public IPs. The format is: *port(range) on external iface:port on internal iface>destination IP.* If a range is specified, all the ports on the external interface will be forwarded incrementally to the portrange specified on the internal interface. (I.E. specify the rule "1-5:2-6>10.0.0.1", port 1 will be forwarded to port 2 on 10.0.0.1, 2 forwards to 3, etc).
- As of 2.3.8-pre3 you will also need to allow them in TCP_ALLOW or similar.
- Remember, these will normally **only** apply to the external interface (INET_IFACE). If you need it to apply to local interfaces as well, you **must** specify a local IP address. If you are trying to get

requests from your lan clients to www.yourdomain.com to get back to your internal server, **run DNS** on the lan to resolve www.yourdomain.com to the internal server's ip.

UDP_FW=""

- Same as above but using UDP (some games may need this, such as older versions of starcraft).

MANGLE_TOS_OPTIMIZE="TRUE"

- This changes the TOS of various packets (mostly generated by games) to ask for special treatment by routers along the way
- Often, this is silently ignored by internet routers, but some can provide different routes for high-bandwidth vs. low-latency (think gigabit satellite link vs. T1).
- This has been known to cause problems; disable if you have problems or just don't like it

DHCP_SERVER="FALSE"

- Set to TRUE if the firewall is also a DHCP server. DHCP clients do not need this. This allows broadcasts to the server from potential clients on the LAN to succeede.

BAD_ICMP="5 9 10 15 16 17 18"

- This is a list of ICMP messages to deny from the internet. Numeric or english form is acceptable. ICMP message types: 0)Echo Reply 1,2)Reserved 3)Destination Unreachable 4)Source Quench 5)Redirect 6)Alternate Host Address 7)No Info 8)Echo Request 9)Router Advertisement 10)Router Solicitation 11)Time Exceeded 12)Parameter Problem 13)Timestamp Request 14)Timestamp Reply 15)Information Request 16)Information Reply 17)Address Mask Request 18)Address Mask Reply 19-29)Reserved 30)Traceroute 31)Conversion Error (The rest are boring).

ENABLE="N"

- You will need to set this to "Y" or it won't run. This is a saftey measure to make sure people don't blindly run it without configuring it.

Flood Parameters Configuration

- **LOG_FLOOD="2/s"**
  - How often to log to the log file if something's happening that has logging on it (the L-policies for DROP, synfloods, ping floods). This is to prevent logs from being filled with duplicate messages. Probably should be decreased unless you are investigating things.
- **SYN_FLOOD="20/s"**
  - Rate at which to allow SYN packets. SYN packets are used in establishing a TCP connection. If you have no services running, you can take this down to 1-5/s and let the burst take care of the occasional FTP, DCC, ICQ, etc connections. Servers will probably need this MUCH higher. If you have problems with connections to your computer failing, increase this number.
  - This is a very ugly way to prevent synfloods. Much better options exist (such as

?Syn Cookies). This is intended to be a "last resort" kind of option (similar to the "! ?Max Clients"

option on Apache), only meant to keep the system from spiraling down into nothingness under the brunt of an insane synflood. Set this option very high.

- **PING_FLOOD="1/s"**
  - How many pings to respond to per second. For most people 1 per second or even less is sufficient (just enough to check to see if you're up). www.yahoo.com might want more though :)

Outbound filters

- **ALLOW_OUT_TCP=""**
  - Internal hosts allowed to be forwarded out on TCP (do not put this/these host/s in INTERNAL_LAN, but do define their method of access (snat or masq) if not a public ip). Use the source luke.
- **PROXY=""**
  - Redirect for Squid or other transparent proxy. Syntax to specify the proxy is "host:port".
- **MY_IP=""**
  - Set to the internal IP of this box (with the firewall). This is only needed when PROXY is used.

Experimental Options (please report your successes/failures)

MAC Address stuff is broken currently; see Mon Motha Known Bugs

- **MAC_MASQ=""**
  - MAC addresses permitted to use masquerading, leave blank to not use"
- **MAC_SNAT=""**
  - MAC addresses permitted to use static NAT, leave blank to not use (format is <MAC Address>:<external ip>)
- **TTL_SAFE=""**
  - How many hops packets need to make once they get on your LAN (null disables the mangling) (requires patch from patch-o-matic). Probably for extremely paranoid people only, it's only in for fun.
- **USE_SYNCOOKIES="FALSE"**
  - TCP

?Syn Cookies on or off (TRUE/FALSE toggle). Recommended to TRUE, because this will protect you from SYN floods by posing a cryptographic challenge per every TCP connection to make illegitimate connections computationally expensive, thus rendering SYN floods mostly ineffective. Requires more CPU power on your firewall machine, though not noticably so unless you have an active server or you are synflooded.

- **SUPER_EXEMPT=""**
  - A list of hosts that get to completely **bypass the packet filter**. Separate with spaces. Use these with **extreme** caution (you might as well add them to /etc/hosts.equiv while you're at it if you trust these hosts this much).
  - ***REMEMBER:*** *IP Addresses can be spoofed!!!!*
- **BRAINDEAD_ISP="FALSE"**
  - This option forces no fragments on TCP. Useful if you have an ISP with a braindead firewall that blocks ICMP fragment needed messages or if you are on a tunneled connection (such

as PPPoE DSL) with an MTU lower than that of your LAN.

- **ALLOW_HOSTWISE_PROTO=””**
  - This option allows you to allow IP protocols (other than UDP and TCP). Note that this has nothing to do with TCP or UDP port numbers. Standard notation is acceptable for a host, so if you want to allow from everyone it is acceptable to use 0/0 for the host to allow from.
- **PROTO_FW=””**
  - This option allows you to forward arbitrary IP protocols to another host. Syntax is “protocol>host<locip”, where protocol may be specified either numerically or through any other means recognized by iptables.

Pre-Alpha and non-functional stuff - Don't bother unless you're working on it.

- **DMZ_IFACE=””**
  - Interface your DMZ is on (leave blank if you don't have one).
  - *DMZ is now obsolete in favor of multiple internet interfaces and will be removed prior to 2.4.0*

Additional information

LOCIP options for configuration directives

Many configuration directives allow a LOCIP option to be specified. This allows you to filter based on the destination IP. This is useful if the system running the firewall has multiple public IPs or you are running publicly routable IPs on your internal LAN and want to open ports to a single host only.

Outbound filtering

The script has very little support for outbound filters. This will be addressed in the later 2.5.x development series (not begun as of 23 June 2002).