在 linux 上可以用 arptables 配置 arp 防火 墙，网上 google 了一下，关于 arptables 的文章没几篇，都是抄来抄去，这两天把 arptables 研究了一把，发现还是很简单的，把配置过程 给大家共享一下。实验环境是 rhel 5u1 32 位。

1. 安装 arptables

arptables 的下载页面是：http://sourceforge.net/projects/ebtables/files/

0.0.3.3 版本的下载链接：http://downloads.sourceforge.net ... les-v0.0.3-3.tar.gz

下载以后安装：

tar zxvf arptables-v0.0.3-3.tar.gz

cd arptables-v0.0.3-3/

make

make install

生 成 的 命 令 是 /usr/local/sbin /arptables 、 /usr/local/sbin/arptables-save 、 /usr/local /sbin/arptables-restore，系统 启动脚本/etc/rc.d/init.d /arptables，这个脚本读的配置文件 必须放在 /etc/sysconfig/arptables 里。

打开 arptables 服务：

chkconfig arptables on

2. 配置 arptables

linux 服务器的网关 MAC 是 00:24:51:E9:C7:10，同网段另一台服务器 192.168.1.10（主机名是 nh-blade-67）的 MAC 地址是 00:17:A4:A8:68:11。

用命令行配置 arp 防火墙：

在 eth0 上如果源 IP 是 192.168.1.10，并且源 MAC 不是 00:17:A4:A8:68:11 的话，就禁止这个数据帧。

/usr/local/sbin/arptables -A INPUT -i eth0 --src-ip 192.168.1.10 --src-mac ! 00:17:A4:A8:68:11 -j DROP

在 eth0 上如果源 MAC 不是 00:24:51:E9:C7:10（网关的 MAC 地址），就禁止这个数据帧，这一条针对外网过来的访问。

/usr/local/sbin/arptables -A INPUT -i eth0 --src-mac ! 00:24:51:E9:C7:10 -j DROP

注意：添加 arp 防火墙策略的次序不能错，针对网关 MAC 地址的语句必须放在最后，否则本网段 IP 的访问策略不能生效。

把以上策略写入配置文件：

/usr/local/sbin/arptables-save > /etc/sysconfig/arptables

/etc/sysconfig/arptables 文件的内容：

*filter

:INPUT ACCEPT

:OUTPUT ACCEPT

:FORWARD ACCEPT

-A INPUT -j DROP -i eth0 -o any -s nh-blade-67 ! --src-mac 00:17:a4:a8:68:11

-A INPUT -j DROP -i eth0 -o any ! --src-mac 00:24:51:e9:c7:10

用命令/etc/init.d/arptables restart 重启 arptables 的时候提示出错：

Stopping Arp filtering (arptables): [OK]

Starting Arp filtering (arptables): arptables v0.0.3-3: Can't use -o with INPUT

Try `arptables -h' or 'arptables --help' for more information.

ERROR(line 5):

[FAILED]

修改/etc/sysconfig/arptables 文件以后的内容：

*filter

:INPUT ACCEPT

:OUTPUT ACCEPT

:FORWARD ACCEPT

-A INPUT -j DROP -i eth0 any -s nh-blade-67 ! --src-mac 00:17:a4:a8:68:11

-A INPUT -j DROP -i eth0 any ! --src-mac 00:24:51:e9:c7:10

再重启 arp 防火墙就没有错误。查看 arp 防火墙状态/etc/init.d/arptables status：

*filter

:INPUT ACCEPT

:OUTPUT ACCEPT

:FORWARD ACCEPT

-A INPUT -j DROP -i eth0 -o any -s nh-blade-67 ! --src-mac 00:17:a4:a8:68:11

-A INPUT -j DROP -i eth0 -o any ! --src-mac 00:24:51:e9:c7:10

注：

RHEL5U1 自带 arptables 的版本是 0.0.8，命令里不能带--source-ip 参数，这个版本不是 sourceforge.net 上发布 的。