layer7 -- l7

应用：xunlei, qq, netfilter<--patch

-m layer7 --l7proto xunlei -j DROP

yum -y install ncurses-devel

下载源代码：

###################################3

当你想实现通过iptables限制迅雷、QQ等应用层协议的时候就需要安装layer7的补丁，而这个补丁的安装涉及到了内核源码编译，打补丁，iptables重新编译的，是个十分好的综合学习过程。本文讲述内核编译和打补丁

介绍：

L7-filter (Application Layer Packet Classifier for Linux), 是 Linux netfilter 的外挂模块, 它能使 Linux 的 iptables 支持 Layer 7 (Application 应用层) 过滤功能, 限制封杀 P2P、即时通讯软件。

过程：

1 内核打补丁，重新编译内核

2 iptables打补丁，重新编译iptables

3 安装l7proto

**1 首先查看内核版本，这个软件对内核版本有要求**

uname -r

**2. 下载所需软件包：**

**kernel 2.6.19.7**

# wget http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.19.7.tar.bz2

**iptables 1.3.7**

# wget http://www.netfilter.org/projects/iptables/files/iptables-1.3.7.tar.bz2

**L7-filter** http://sourceforge.net/project/showfiles.php?group\_id=80085

netfilter-layer7-v2.12.tar.gz

l7-protocols-2007-06-22.tar.gz

**3. 配置编译新内核**

首先将所下载的软件都放置于/usr/src目录下

# tar zxvf netfilter-layer7-v2.12.tar.gz

# tar xjvf linux.2.6.19.7.tar.bz2

**# ln -s linux.2.6.19.7 linux**

# cd linux

# patch -p1 < /usr/src/netfilter-layer7-v2.9/kernel-2.6.18-2.6.19-layer7-2.9.patch (打L7-filter的内核补丁)

# make oldconfig

(如果之前曾经编译过，需要先执行 make mrproper 。make oldconfig会自动对比之前的kernel config，根据之前版本的配置生成一个kernel config，这样方便我们在编译新核心的时候，无须在从头修改所有的核心设置）

# make menuconfig 设定内核参数 如果出错可能是因为未安装 ncurses-devel

核心不同，内核选项的排列方式有可能不一样，仔细找一下可以找到：

Code maturity level options –> [\*] Prompt for development and/or incomplete code/drivers

Networking –> Networking options –>

[\*] Network packet filtering (replaces ipchains) –>

IP: Netfilter Configuration –>

<M> Connection tracking (required for masq/NAT)

[\*] Connection tracking flow accounting

<M> IP tables support (required for filtering/masq/NAT)

<M> Layer 7 match support

# make 时间消耗长

# make modules

# make modules\_install

# make install

# reboot

# uame -a

Linux jason.10235 2.6.19.7 #1 Fri Jul 6 11:56:11 CST 2007 i686 i686 i386 GNU/Linux

系统已经更新至新内核 2.6.19.7

**4. 更新升级Iptalbes的Layer7补丁（注意备份iptables规则）**

# cd /usr/src

# tar xjvf iptables-1.3.7.tar.bz2

# cd iptables-1.3.7

# patch -p < ../netfilter-layer7-v2.0/iptables-layer7-2.0.patch

# chmod +x extensions/.layer7-test

# export KERNEL\_DIR=/usr/src/linux-2.6.19.7

# export IPTABLES\_DIR=/usr/src/iptables-1.3.7

# make BINDIR=/sbin LIBDIR=/lib MANDIR=/usr/share/man install

# iptables -V

iptables v1.3.7 已经更新至新版本

**5. 安装Layer7 协议文件**

# cd /usr/src

# tar zxvf l7-protocols-2007-06-22.tar.gz

# cd l7-protocols-2007-06-22

# make install

**6. 使用iptables layer-7 filter：**

# iptables -t mangle -I PREROUTING -m layer7 --l7proto edonkey -j DROP (禁止edonkey)

# iptables -t mangle -I PREROUTING -m layer7 --l7proto bittorrent -j DROP (禁止bt)

# iptables -t mangle -I PREROUTING -m layer7 --l7proto qq -j DROP (禁止QQ通讯)

# iptables -t mangle -I PREROUTING -m layer7 --l7proto msnmessenger -j DROP (禁止edonkey)

# iptables -t mangle -I PREROUTING -m layer7 --l7proto xunlei -j DROP (禁止迅雷)

# iptables -t mangle -I PREROUTING -m layer7 --l7proto kugoo -j DROP (禁止kugoo)

# iptables -t mangle -I PREROUTING -m layer7 --l7proto yahoo -j DROP (禁止Yahoo! Messenger)

例子：

禁MSN传送文件的方法

iptables 七层实现的。

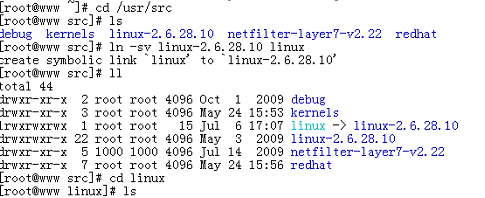
iptables -A FORWARD -m layer7 --l7proto msn-filetransfer -j DROP

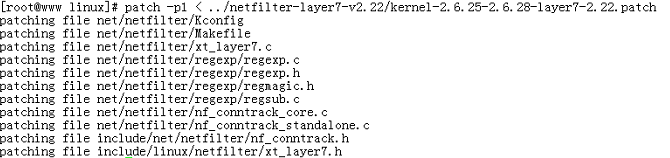
先解压内核到

tar xf linux…. -C /usr/src

tar xf netfilter-layer7-…. -C /usr/src

cd /









选择：

Kernel Patch

# tar zxvf linux-2.6.28.10.tar.gz -C /usr/src

# tar zxvf netfilter-layer7-v2.22.tar.gz -C /usr/src

# cd /usr/src

# ln –s linux-2.6.28.10 linux

# cd /usr/src/linux/

# patch -p1 < ../netfilter-layer7-v2.22/kernel-2.6.25-2.6.28-layer7-2.22.patch

# cp /boot/config-2.6.18-164.el5 /usr/src/linux/.config

# make menuconfig

Networking support → Networking Options →Network packet filtering framework →Core Netfilter Configuration

<M> Netfilter connection tracking support

<M> “layer7” match support

<M> “string” match support

<M> “time” match support

<M> “iprange” match support

<M> “connlimit” match support

<M> “state” match support

<M> “conntrack” connection match support

<M> “mac” address match support

<M> "multiport" Multiple port match support

Networking support → Networking Options →Network packet filtering framework → IP: Netfilter Configuration

<M> IPv4 connection tracking support (required for NAT)

<M> Full NAT

<M> MASQUERADE target support

<M> NETMAP target support

<M> REDIRECT target support

# make

# make modules\_install

# make install

Compiles iptables :

# cp /etc/init.d/iptables ~/iptables

# cp /etc/sysconfig/iptables-config ~/

# rpm -e iptables-ipv6 iptables iptstate --nodeps

# tar jxvf iptables-1.4.6.tar.bz2 –C /usr/src

# cd /usr/src/iptables-1.4.6

#cp../netfilter-layer7-v2.22/iptables-1.4.3forward-for-kernel-2.6.20forward/libxt\_layer7.\* ./extensions/

# ./configure --prefix=/usr --with-ksource=/usr/src/linux

# make

# make install

# tar zxvf l7-protocols-2009-05-28.tar.gz

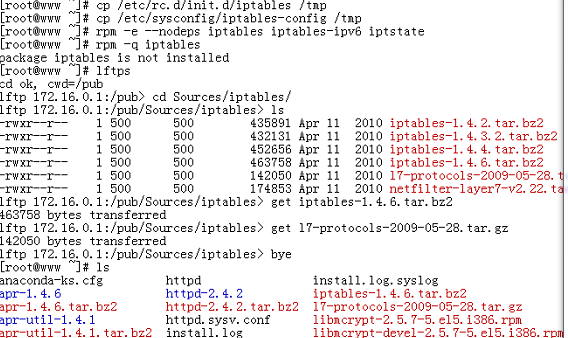
# cd l7-protocols-2009-05-28

# make install

# mv ~/iptables /etc/rc.d/init.d/

# service iptables start

注意



l7-filter uses the standard iptables extension syntax

# iptables [specify table & chain] -m layer7 --l7proto [protocol name] -j [action]