實作 Layer 7 封包過濾

參考資訊

- L7-filter Kernel Version HOWTO
- L7-filter 安裝實錄

下載檔案

要手動編譯新版本的核心並加入 layer7 封包過濾選項的話，需要俱備以下套件：

- linux kernel source
- iptables source
- l7-filter patch
- l7-filter protocols

在本文當中，所重新編譯的版本如下：

- kernel：2.6.24.4
- iptables：1.4.0
- l7-filter patch：2.17
- l7-filter protocols：2008-02-20

為了方便管理，把以上套件均放在 /usr/src/kernels。

```
root # cd /usr/src/kernels/
```

可以選擇任何可下載網路檔案的工具，如 lynx、wget，或 mozilla、firefox 等等工具下載，在此範例使用 wget，方法如下：

```
root # wget
ftp://ftp.tw.kernel.org/pub/linux/kernel/v2.6/linux-2.6.24.4.tar.bz2
root # wget
ftp://ftp.netfilter.org/pub/iptables/iptables-1.4.0.tar.bz2
root # wget
http://nchc.dl.sourceforge.net/sourceforge/l7-filter/netfilter-layer7
-v2.17.tar.gz
root # wget
http://nchc.dl.sourceforge.net/sourceforge/l7-filter/l7-protocols-200
8-02-20.tar.gz
```

將套件解壓縮。

```
root # tar -jxvf linux-2.6.24.4.tar.bz2; \
> tar -zxvf l7-protocols-2008-02-20.tar.gz; \
> tar -zxvf netfilter-layer7-v2.17.tar.gz; \
> tar -jxvf iptables-1.4.0.tar.bz2
```

更新 kernel

為了安裝方便，我們為 linux-2.6.24.4 這個目錄建位一個軟連結，以便切換目錄。

更新 kernel patch，增加 layer7 filter 選項。

```
root # ln -s linux-2.6.24.4 linux; cd linux
```

若您想延續使用舊版 kernel 的選項的話，您可以把 .config 檔案複制到新 kernel 的目錄下，此時重新選擇項目時就會延用之前的設定。

為 kernel source 上 layer7 的 patch。

```
root # patch -p1
< ../netfilter-layer7-v2.17/kernel-2.6.22-2.6.24-layer7-2.17.patch
patching file net/netfilter/Kconfig
patching file net/netfilter/Makefile
patching file net/netfilter/xt_layer7.c
patching file net/netfilter/regexp/regexp.c
patching file net/netfilter/regexp/regexp.h
patching file net/netfilter/regexp/regmagic.h
patching file net/netfilter/regexp/regsub.c
patching file net/netfilter/nf_conntrack_core.c
patching file net/netfilter/nf_conntrack_standalone.c
patching file include/net/netfilter/nf_conntrack.h
patching file include/linux/netfilter/xt_layer7.h
```

選擇 layer 7 相關選項

在 kernel 選項裡，需要把相關的設定選擇起來才可以，以下為完整有關 layer 7 的項目。

```
root # make menuconfig
 General setup  --->
    [*] Prompt for development and/or incomplete code/drivers
 Networking  --->
      Networking options  --->
         [*] Network packet filtering framework (Netfilter)  --->
              Core Netfilter Configuration  --->
                 <M> Netfilter connection tracking support
                 -*- Connection tracking flow accounting
                 -*- Connection mark tracking support
                 [*] Connection tracking security mark support
                 [*] Connection tracking events (EXPERIMENTAL)
                 <M> SCTP protocol connection tracking support
                 <M> UDP-Lite protocol connection tracking support
```

```
<M> Amanda backup protocol support
<M> FTP protocol support
<M> H.323 protocol support (EXPERIMENTAL)
<M> IRC protocol support
<M> NetBIOS name service protocol support
<M> PPtP protocol support
<M> SANE protocol support (EXPERIMENTAL)
<M> SIP protocol support (EXPERIMENTAL)
<M> TFTP protocol support
<M> Connection tracking netlink interface
{M} Netfilter Xtables support (required for ip_tables)
<M>   "CLASSIFY" target support
<M>   "CONNMARK" target support
<M>   "DSCP" target support
<M>   "MARK" target support
<M>   "NFQUEUE" target Support
<M>   "NFLOG" target support
<M>   "NOTRACK" target support
<M>   "TRACE" target support
<M>   "TRACE" target support
<M>   "SECMARK" target support
<M>   "CONNSECMARK" target support
<M>   "TCPMSS" target support
<M>   "comment" match support
<M>   "connbytes" per-connection counter match support
<M>   "connlimit" match support"
<M>   "connmark" connection mark match support
<M>   "conntrack" connection tracking match support
<M>   "DCCP" protocol match support
<M>   "DCCP" protocol match support
<M>   "DSCP" match support
<M>   "ESP" match support
<M>   "helper" match support
<M>   "length" match support
<M>   "limit" match support
<M>   "mac" address match support
<M>   "mark" match support
<M>   IPsec "policy" match support
```

```
    <M>   Multiple port match support
    <M>   "physdev" match support
    <M>   "pkttype" packet type match support
    <M>   "quota" match support
    <M>   "realm" match support
    <M>   "sctp" protocol match support (EXPERIMENTAL)
    <M>   "state" match support
    <M>   "layer7" match support
    [*]     Layer 7 debugging output
    <M>   "statistic" match support
    <M>   "string" match support
    <M>   "tcpmss" match support
    <M>   "time" match support
    <M>   "u32" match support
    <M>   "hashlimit" match support
  IP: Netfilter Configuration  --->
    <M> IPv4 connection tracking support (required for NAT)
    [*]   proc/sysctl compatibility with old connection
    <M>  IP Userspace queueing via NETLINK (OBSOLETE)
    <M> IP tables support (required for filtering/masq/NAT)
    <M>   IP range match support
    <M>   TOS match support
    <M>   recent match support
    <M>   ECN match support
    <M>   AH match support
    <M>   TTL match support
    <M>   Owner match support
    <M>   address type match support
    <M>   Packet filtering
    <M>     REJECT target support
    <M>   LOG target support
    <M>   ULOG target support
    <M>   Full NAT (NEW)
    <M>     MASQUERADE target support
    <M>     REDIRECT target support
    <M>     NETMAP target support
    <M>     SAME target support (OBSOLETE)
    <M>     Basic SNMP-ALG support (EXPERIMENTAL)
```

```
                <M>   Packet mangling
                <M>     TOS target support
```

較為重要的是 "layer7" match support 項目與 IPv4 connection tracking support (required for NAT) 項目，若您不知道的話就請把 Core Netfilter Configuration 與 IP: Netfilter Configuration 裡的選項全部選起來即可。

編譯並安裝新版核心

重 kernel 2.6 開始，編譯核心就變得更為簡單，只需要幾個 make 的指令即可，安裝完後會自動修改 GRUB 的選項，不需手動修改，減少了手動修改錯誤的危險。

```
root # make
root # make modules
root # make modules_install
root # make install
sh /usr/src/kernels/linux-2.6.24.4/arch/x86/boot/install.sh 2.6.24.4
arch/x86/boot/bzImage System.map "/boot"
```

更新 iptables patch

更新 iptables 需注意是否在現有的 kernel 中 netfilter 子系統相符合，若使用了不在 kernel 所支援的模組，在設定 iptables 會出現錯誤。以下指令可新增 laery7 模組的指令。

```
root # cd /usr/src/kernels/iptables-1.4.0
root # patch -p1
< ../netfilter-layer7-v2.17/iptables-1.4-for-kernel-2.6.20forward-layer7-2.17.patch
patching file extensions/libipt_layer7.c
patching file extensions/libipt_layer7.man
patching file extensions/.layer7-test
```

設定 KERNEL_DIR 與 IPTABLES_DIR 環境變數，並開始編譯安裝。

```
root # export KERNEL_DIR=/usr/src/kernels/linux;
root # export IPTABLES_DIR=/usr/src/kernels/iptables-1.4.0
root # chmod +x extensions/.layer7-test
root # make && make install
```

安裝通訊定議檔

使用 layer7 模組時，會參考 /etc/l7-protocols 目錄下的定議檔，各通訊協定的封包特徵會在 l7-protocols 的套件裡，解開之後直接安裝即可。

```
root # cd /usr/src/kernels/l7-protocols-2008-02-20
root # make install
mkdir -p /etc/l7-protocols
cp -R * /etc/l7-protocols
```

重新開機

重新編譯了核心之後，需要重新啟動電腦才能套用新的核心套件，請使用 uname 指令查看是否設定成功。

```
root # uname -a; iptables -V
Linux localhost.localdomain 2.6.24.4 #1 SMP Thu Apr 10 23:21:08 CST 2008 i686 i686 i386 GNU/Linux
iptables v1.4.0
```

測試

MSN Messenger

以下測試會拒絕連出 MSN Menssenger 封包，在 iptables 的 OUTPUT 政策裡，我們在 X-Window 執行 GAIM 連出時，會發現 msnmessenger 的封包被 DROP。

語法：

```
iptables -A OUTPUT -m layer7 --l7proto msnmessenger -j DROP
```

```
root # iptables -A OUTPUT  -m layer7 --l7proto msnmessenger -j DROP
root # iptables -L -n -v
Chain INPUT (policy ACCEPT 3056 packets, 394K bytes)
pkts    bytes   target  prot    opt in  out source  destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts    bytes   target  prot    opt in  out source  destination

Chain OUTPUT (policy ACCEPT 1274 packets, 159K bytes)
pkts  bytes target  prot opt  in out  source    destination
34  2584    DROP    all  --   *  *    0.0.0.0/0  0.0.0.0/0    LAYER7
    l7proto msnmessenger
```

BitTorrent

第二個測試拒絕連出 BitTorrent 封包，我們在設定好拒絕 bittorrent 封包後，在本機使用 BT 下載檔案均失敗，可從 iptables 指令查出。

語法：

```
iptables -A OUTPUT -m layer7 --l7proto bittorrent -j DROP
```

```
root # iptables -A OUTPUT  -m layer7 --l7proto bittorrent -j DROP
root # iptables -L -n -v
Chain INPUT (policy ACCEPT 3056 packets, 394K bytes)
pkts    bytes   target  prot    opt in  out source  destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts    bytes   target  prot    opt in  out source  destination

Chain OUTPUT (policy ACCEPT 1274 packets, 159K bytes)
pkts  bytes target  prot opt  in out  source    destination
34    2584  DROP    all  --   *  *    0.0.0.0/0  0.0.0.0/0    LAYER7
l7proto msnmessenger
78    7920  DROP    all  --   *  *    0.0.0.0/0  0.0.0.0/0    LAYER7
l7proto bittorrent
```

若您把 layer7 安裝在網路閘道 (Gateway) 上的話，那麼請使用 PREROUTING 或 FORWARD 連線才會有效。iptables 可參考 iptables 封包過濾規則 (new window)。

後記

若您打算在您的防火牆上使用 layer7 封包過濾功能的話，那麼所需的記憶體與 CPU 會更多，若您的使用者連線數同一時間超過百人，並且頻繁的取存網路的話，那麼可能需要考慮使用較高效能的網路卡與更多的記憶體。

若您在啟用 layer7 功能後發現網路變得很慢的話，那麼就需要檢查您的網卡與記憶體是否足夠。

For more articles, please visit http://ms.ntcb.edu.tw/~steven/

作者：廖子儀 (Tzu-Yi Liao)
Certified：LPIC Level I、LPIC Level II、RHCE
E-mail：steven@ms.ntcb.edu.tw
Web site：Steven's Linux Note (http://ms.ntcb.edu.tw/~steven/)