Firewall dengan Menggunakan iptables

IPTables merupakan salah satu firewall popular dan powerfull yang tersedia di sistem operasi Linux. Artikel ini akan menuturkan setup dasar dan konfigurasi IPTables untuk distribusi GNU/Linux pada umumnya.

Rekruitmen

Sebuah komputer dengan prosessor 586 atau lebih tinggi, RAM 128mb, dua buah netcard, hard drive 2 GB atau yang berkapasitas lebih besar, Sistem Operasi Linux.

Konfigurasi Kernel

Anda akan perlu menambahkan beberapa opsi di file konfigurasi kernel :

```
#
# IP: Netfilter Configuration
#
CONFIG_IP_NF_CONNTRACK=y
CONFIG_IP_NF_CT_ACCT=y
CONFIG_IP_NF_CONNTRACK_MARK=y
CONFIG_IP_NF_CT_PROTO_SCTP=y
CONFIG_IP_NF_FTP=y
CONFIG_IP_NF_IRC=y
CONFIG_IP_NF_TFTP=y
CONFIG_IP_NF_AMANDA=y
CONFIG_IP_NF_QUEUE=y
CONFIG_IP_NF_IPTABLES=y
CONFIG_IP_NF_MATCH_LIMIT=y
CONFIG_IP_NF_MATCH_IPRANGE=y
CONFIG_IP_NF_MATCH_MAC=y
CONFIG_IP_NF_MATCH_PKTTYPE=y
CONFIG_IP_NF_MATCH_MARK=y
CONFIG_IP_NF_MATCH_MULTIPORT=y
CONFIG_IP_NF_MATCH_TOS=y
CONFIG_IP_NF_MATCH_RECENT=y
CONFIG_IP_NF_MATCH_ECN=y
CONFIG_IP_NF_MATCH_DSCP=y
CONFIG_IP_NF_MATCH_AH_ESP=y
CONFIG_IP_NF_MATCH_LENGTH=y
CONFIG_IP_NF_MATCH_TTL=y
CONFIG_IP_NF_MATCH_TCPMSS=y
CONFIG_IP_NF_MATCH_HELPER=y
CONFIG_IP_NF_MATCH_STATE=y
CONFIG_IP_NF_MATCH_CONNTRACK=y
CONFIG_IP_NF_MATCH_OWNER=y
CONFIG_IP_NF_MATCH_ADDRTYPE=y
CONFIG_IP_NF_MATCH_REALM=y
CONFIG_IP_NF_MATCH_SCTP=y
CONFIG_IP_NF_MATCH_COMMENT=y
CONFIG_IP_NF_MATCH_CONNMARK=y
```

```
CONFIG_IP_NF_MATCH_HASHLIMIT=y
CONFIG_IP_NF_FILTER=y
CONFIG_IP_NF_TARGET_REJECT=y
CONFIG_IP_NF_TARGET_LOG=y
CONFIG_IP_NF_TARGET_ULOG=y
CONFIG_IP_NF_TARGET_TCPMSS=y
CONFIG_IP_NF_NAT=y
CONFIG_IP_NF_NAT_NEEDED=y
CONFIG_IP_NF_TARGET_MASQUERADE=y
CONFIG_IP_NF_TARGET_REDIRECT=y
CONFIG_IP_NF_TARGET_NETMAP=y
CONFIG_IP_NF_TARGET_SAME=y
CONFIG_IP_NF_NAT_LOCAL=y
CONFIG_IP_NF_NAT_SNMP_BASIC=y
CONFIG_IP_NF_NAT_IRC=y
CONFIG_IP_NF_NAT_FTP=y
CONFIG_IP_NF_NAT_TFTP=y
CONFIG_IP_NF_NAT_AMANDA=y
CONFIG_IP_NF_MANGLE=y
CONFIG_IP_NF_TARGET_TOS=y
CONFIG_IP_NF_TARGET_ECN=y
CONFIG_IP_NF_TARGET_DSCP=y
CONFIG_IP_NF_TARGET_MARK=y
CONFIG_IP_NF_TARGET_CLASSIFY=y
CONFIG_IP_NF_TARGET_CONNMARK=y
CONFIG_IP_NF_TARGET_CLUSTERIP=y
CONFIG_IP_NF_RAW=y
CONFIG_IP_NF_TARGET_NOTRACK=y
CONFIG_IP_NF_ARPTABLES=y
CONFIG_IP_NF_ARPFILTER=y
CONFIG_IP_NF_ARP_MANGLE=y
```

Atau bila menggunakan konfigurasi dengan menu, anda akan menemukan opsi tersebut pada bagian berikut :

```
Device Drivers  --->
|_Networking support  --->
  |_Networking options  --->
    |_Network packet filtering --->
      |_IP: Netfilter Configuration  --->
        <*> Connection tracking (required for masq/NAT)
        [*]   Connection tracking flow accounting
        [*] Connection mark tracking support
        <*> SCTP protocol connection tracking support (EXPERIMENTAL)
        <*> FTP protocol support
        <*> IRC protocol support
        <*> TFTP protocol support
        <*> Amanda backup protocol support
        <*> Userspace queueing via NETLINK
        <*> IP tables support (required for filtering/masq/NAT)
        <*>   limit match support
        <*>   IP range match support
        <*>   MAC address match support
        <*>   Packet type match support
```

```
<*>  netfilter MARK match support
<*>  Multiple port match support
<*>  TOS match support
<*>  recent match support
<*>  ECN match support
<*>  DSCP match support
<*>  AH/ESP match support
<*>  LENGTH match support
<*>  TTL match support
<*>  tcpmss match support
<*>  Helper match support
<*>  Connection state match support
<*>  Connection tracking match support
<*>  Owner match support
<*>  address type match support
<*>  realm match support
<*>  SCTP protocol match support
<*>  comment match support
<*>  Connection mark match support
<*>  hashlimit match support
<*>  Packet filtering
<*>    REJECT target support
<*>  LOG target support
<*>  ULOG target support
<*>  TCPMSS target support
<*>  Full NAT
<*> MASQUERADE target support
<*> REDIRECT target support
<*> NETMAP target support
<*> SAME target support
[*] NAT of local connections (READ HELP)
<*> Basic SNMP-ALG support (EXPERIMENTAL)
```

Jika telah selesai konfigurasi kernel, compile kernel, dan install kernel. Kini install'lah paket Iptables. Pada Mandrake *"urpmi iptables"*, di debian *"apt-get install iptables"*, di gentoo dari ports *"emerge iptables"*, untuk suse *"yast -i iptables"*. Setelah paket Iptables terinstall, kita perlu memastikan jika "IP forwarding" telah "enable" di kernel, kecuali jika anda menginginkan komputer anda tidak berlaku sebagai router/NAT.

Aktifkan IP fowarding dengan menambahkan baris berikut di /etc/sysctl.conf

```
net.ipv4.ip_forward = 1
```

Aturan Iptables

Contoh berikut adalah script shell yang sangat sederhana dengan aturan membolehkan seluruh trafik keluar dari jaringan internal dan hanya beberapa port saja yang dapat diakses dari jaringan eksternal. Diasumsikan kita menggunakan **eth0**

sebagai interface eksternal dan **eth1** sebagai interface internal, sesuaikan variabel **EXTIF** dan **INTIF** tersebut pada komputer anda. Buatlah file baru dengan nama *firewall* yang berisi script sebagai berikut.

```
#!/bin/sh
IPTABLES='/sbin/iptables'

# Set nilai interface
EXTIF='eth0'
INTIF='eth1'

#Aktifkan ip forwarding di kernel
/bin/echo 1 > /proc/sys/net/ipv4/ip_forward

#flush aturan dan hapus chains
$IPTABLES -F
$IPTABLES -X

#Aktifkan masquerade untuk membolehkan LAN mengakses jaringan  eksternal
$IPTABLES -t nat -A POSTROUTING -o $EXTIF -j MASQUERADE

#Tersukan trafik LAN dari LAN $INTIF ke internet $EXTIF
$IPTABLES -A FORWARD -i $INTIF -o $EXTIF -m state --state NEW,ESTABLISHED -j ACCEPT
#Membolehkan akses ke server SSH
$IPTABLES -A INPUT --protocol tcp --dport 22 -j ACCEPT

#Membolehkan akses ke server HTTP
$IPTABLES -A INPUT --protocol tcp --dport 80 -j ACCEPT

#blok seluruh akses ke $EXTIF
$IPTABLES -A INPUT -i $EXTIF -m state --state NEW,INVALID -j DROP
$IPTABLES -A FORWARD -i $EXTIF -m state --state NEW,INVALID -j DROP


#Alihkan port TCP 25 ke komputer lain pada jaringan internal
$IPTABLES -A FORWARD -i $EXTIF -d 10.0.0.5 -p tcp --dport 25 -j ACCEPT
$IPTABLES -t nat -A PREROUTING -i $EXTIF -p tcp --dport 25 -j DNAT --to-destination 10.0.0.6:25
```

Kini jalankan service IPTables sehingga aturan tadi bisa di terapkan.

```
root@host # /etc/init.d/iptables start
* Loading iptables state and starting firewall...       [ ok ]
* Restoring iptables ruleset                           [ ok ]

root@host #chmod +x firewall
root@host #./firewall
```

Agar aturan tersebut tersimpan permanen, ketikkan perintah berikut :

```
root@host # /etc/init.d/iptables save
* Saving iptables state...                    [ ok ]
```

Maka setiap anda reboot, aturan IPTables tadi akan diterapkan secara otomatis.

Semoga Bermanfaat.
Faiz GP
faiz@purwakarta.org