Iptables for dummies

Netfilter

Elke Linux distributie gebruikt Netfilter (in de kernel) voor firewalling. De beheertool daarvoor is '**iptables**', via de commandline.

Hoe werkt het? Er zijn drie soorten verkeer: INPUT, OUTPUT en FORWARD. Dit worden ook wel '**chains**' genoemd.

- INPUT is alles op je interface binnenkomt
- OUTPUT is alles wat je interface verlaat
- FORWARD is als de computer als router is geconfigureerd, dus met meerdere netwerkkaarten

Om te beginnen, moeten we de firewall service stoppen. Op openSUSE is dat

```
rcSuSEfirewall2 stop
```

controle

Vervolgens beginnen we met een schone lei. Verwijder alle firewall regels

```
iptables -F
```

Controleer dit met

```
iptables -L -v
```

dichtzetten

Hierna staat je firewall uit en is leeg, dus we gaan hem snel dichtzetten. We gebruiken hiervoor '**policies**'.

```
iptables -p INPUT DROP
iptables -p OUTPUT DROP
iptables -p FORWARD DROP
```

-p betekent hier policy, INPUT is de chain waarop hij werkt, en de '**target**' is '**drop**'.

targets

Er zijn de volgende targets:

- DROP: alle pakketjes worden gedropt, er is geen terugmelding
- REJECT: het pakketje wordt verworpen, er gaat wel een melding terug
- ACCEPT: het pakketje wordt geaccepteerd
- LOG: er wordt een melding in syslog geschreven over het binnenkomende pakketje

Nu is de computer potdicht, en er is dus niet mee te werken met communicatie naar buiten. We gaan hem zo inrichten dat er communicatie naar buiten mogelijk is.

loopback goedzetten

Maar eerst moet er de loopback interface (lo) goed geconfigureerd worden. Hoewel niet strikt noodzakelijk, maar dit zorgt ervoor dat een hoop zaken goed verlopen.

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```

-A betekent 'append', aan het eind. De volgorde van de regels is belangrijk! De eerste 'hit' wordt uitgevoerd en er wordt daarna niet meer verder gekeken.

-i is de interface

-j (jump) naar welke target

Hierna kan er gepinged worden naar de loopbackinterface:

```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.034 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.019 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.027 ms
```

uitgaand verkeer toestaan

We gaan nu alle uitgaande verkeer toestaan.

`iptables -A OUTPUT -o eth0 -j ACCEPT`

Dit zorgt voor uitgaande pakketjes, maar antwoorden hierop die binnenkomen, kunnen nog steeds niet de computer bereiken.

`iptables -A INPUT -m state - state=ESTABLISHED,RELATED -j ACCEPT`

creert een stateful filter.

Revision #3
Created 2026-04-01 17:12:52 CEST by Philip
Updated 2026-04-13 19:27:20 CEST by Philip