Firewall på router på Ubuntu.

Lige nu kan alle komme på vores router fra den røde side. Det er jo ikke helt godt. At alle på det store WWW, også de ”onde” Blackhat hackers, kan komme på vores router!

Det må vi hellere ændre, så det kun er brugere der sidder fysisk på indersiden af routeren (Det grønne interface) kan komme på vores router. Det gør vi ved at tilføje/ændre i vores iptables firewall.

Hvis du vil undgå at få afbrudt din forbindelse til routeren, udføres kommandoerne fra INDERSIDEN (den grønne side). Sidst i løsningen kommer der et shell script der kan bruges til at indlæse alle følgende kommandoer, og et shellscript der kan bruges til at nulstille router tilbage til kun at route, uden nogen begrænsninger.

I de listede kommandoer herunder gælder følgende (Markeret tekst tilrettes til egen routers rød og grøn interface navn, Dette er mine interfacenavne):

```
Indersiden(Grøn): ins19
Ydersiden(Rød)  : ins18
```

VIGTIG!!! Rækkefølgen på nedenstående reger ER VIGTIGE!!!

Vi starter med at slette alle eksisterende regler, så vi kan begynde på en frisk, med følgende kommandoer. Vær opmærksom på at dette afbryder forbindelse igennem routeren!!!

```
iptables -F
iptables -t nat -F
iptables -t mangle -F
iptables -X
```

Vi starter med at sørge for at loopback trafik altid kommer igennem.

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

Nu må vi også hellere sørge for at vores trafik fra de forbindelser vi sætter i gang fra vores klienter, også kan få et svar til bage igen. (f.eks. tv2.dk kan sende os deres hjemmeside).

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -m state --state NEW ! -i ens18 -j ACCEPT
iptables -A FORWARD -i ens18 -o ens19 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Men det er måske også en god ide at tillade den trafik der tillader udgående forbindelser fra vores inderside.

```
iptables -A FORWARD -i ens19 -o ens18 -j ACCEPT
```

Og vi må hellere også huske vores nat/pat, i form af en Ubuntu iptables `MASQUERADE` kommando:

```
iptables -t nat -A POSTROUTING -o ens18 -j MASQUERADE
```

Det er nok en god ide også at spærre for uønsket trafik ind igennem vores router. Det gør vi at vi ved at den trafik der ikke passer med ovenstående regler, ikke kan komme igennem vores yderside, eller Røde, forbindelse.

```
iptables -A FORWARD -i ens18 -o ens18 -j REJECT
```

Og vi vil heller ikke tillade forbindelser direkte til routeren fra ydersiden (rødt interface):

```
iptables -A INPUT -i ens18 -j DROP
```

Så er vores Firewall færdig, og du burde stadig kunne få forbindelse til router fra indersiden (Grøn), og ingen kan få forbindelse til din router fra ydersiden (Rød).

I stedet for at indtaste hver kommando, er her et script, der kan køres i stedet.

Først rediger en fil, f.eks. en der hedder fireswall.sh

```
nano foreswall.sh
```

Derefter indsæt følgende linjer i filen:

```
#!/bin/sh
PATH=/usr/sbin:/sbin:/bin:/usr/bin
sleep 5
#
# Indersiden ins19
# Ydersiden ins18
#
#
# Slet alle eksiterende regler.
iptables -F
iptables -t nat -F
iptables -t mangle -F
iptables -X
#
# Altid accepter loopback trafik
iptables -A INPUT -i lo -j ACCEPT
#
# Tillad established connections, men kun dem der kommer fra vores inderside (Grøn
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -m state --state NEW ! -i ens18 -j ACCEPT
iptables -A FORWARD -i ens18 -o ens19 -m state --state ESTABLISHED,RELATED -j ACCEPT
#
# tillad udgående connections fra LAN side.
iptables -A FORWARD -i ens19 -o ens18 -j ACCEPT
#
# Opsætning af Masquerade.
iptables -t nat -A POSTROUTING -o ens18 -j MASQUERADE
#
# Ikke send trafik fra ydersiden til indersiden.
iptables -A FORWARD -i ens18 -o ens18 -j REJECT
#
# Kontakt til router fra ydersiden ikke tilladt
iptables -A INPUT -i ens18 -j DROP
```

For at gemme ændringer trykkes der CTRL+S og så CTRL+X, og man er tilbage i prompten.

Nu må vi lige lave vores fil executable (kunne udføre/køre filen) det gør vi sådan her:

```
chmod +x fireswall.sh
```

Så kører vi filen som sudo (HUSK Kør filen fra GUI PC inde på det lukkede netværk!!)

```
sudo ./firewall.sh
```

For at nulstille firewall, så den kun router, kan følgende kommandoer sættes ind i en ny shell fil på vores Router, husk at gøre filen exekverbar:

```
#!/bin/sh
PATH=/usr/sbin:/sbin:/bin:/usr/bin
sleep 5
#
# delete all existing rules.
iptables -F
iptables -t nat -F
iptables -t mangle -F
iptables -X
#
sudo iptables -t nat -A POSTROUTING -o ens18 -j MASQUERADE
```

HUSK!: Når du har udført kommandoer i din firewall at gemme opsætningen, ellers er reglerne slettet og ikke aktive efter genstart af router. Se også vejledning 25 for at gemme opsætning.