```
#enp0s2 = OUTSIDE

#enp0s3 = INSIDE

#poistaa kaikki säännöt

iptables -F

#ALETAAN lisämään palveluja
#lisää sallivat säännöt


iptables -A FORWARD -i enp0s2 -d 10.10.10.5 -p TCP --dport 80 -j ACCEPT
iptables -A FORWARD -i enp0s2 -d 10.10.10.5 -p TCP --dport 433 -j ACCEPT

iptables -A FORWARD -i enp0s3 -s 10.10.10.5 -p TCP --sport 80 -j ACCEPT
iptables -A FORWARD -i enp0s3 -s 10.10.10.5 -p TCP --sport 433 -j ACCEPT


#Salli ICMP  In->Out


iptables -A FORWARD -i enp0s2 -p ICMP --icmp-type=0 -j ACCEPT
iptables -A FORWARD -i enp0s3 -p ICMP --icmp-type=8 -j ACCEPT

#SALLI DNS

iptables -A FORWARD -i enp0s2 -p UDP --sport 53 -j ACCEPT
iptables -A FORWARD -i enp0s3 -p UDP --dport 53 -j ACCEPT

#Salli 80 ja 443 IN ->out

iptables -A FORWARD -i enp0s2 -p TCP --sport 443 -j ACCEPT
iptables -A FORWARD -i enp0s3 -p TCP --dport 443 -j ACCEPT

iptables -A FORWARD -i enp0s2 -p TCP --sport 80 -j ACCEPT
iptables -A FORWARD -i enp0s3 -p TCP --dport 80 -j ACCEPT

#Salli SQL Warehouse -> 10.10.10.5

iptables -A FORWARD -i enp0s2 -p TCP -s 10.10.20.0/24 -d 10.10.10.5 --dport 3306 -j ACCEPT
iptables -A FORWARD -i enp0s3 -p TCP -s 10.10.10.5 -d 10.10.20.0/24 --dport 3306 -j ACCEPT
```

```
#Salli SQL Warehouse -> 10.10.10.5

iptables -A FORWARD -i enp0s2 -p TCP -s 10.10.20.0/24 -d 10.10.10.5 --dport 3306 -j ACCEPT
iptables -A FORWARD -i enp0s3 -p TCP -s 10.10.10.5 -d 10.10.20.0/24 --dport 3306 -j ACCEPT

#salli dns warehouse-office

iptables -A FORWARD -i enp0s2 -p UDP -d 10.10.10.10 -s 10.10.20.0/24 --dport 53 -j ACCEPT
iptables -A FORWARD -i enp0s3 -p UDP -s 10.10.10.10 -d 10.10.20.0/24 --sport 53 -j ACCEPT

#pudottaa kaikki muut paketit jotka tulee outsidestä

iptables -A FORWARD -i enp0s2 -j DROP

#pudottaa kaikki muut paketit jotka tulee insidestä

iptables -A FORWARD -i enp0s3 -j DROP
```

Stateless firewall

#eth0 = OUTSIDE

#eth1 = INSIDE

#removes all rules

iptables -F

#Allow http ja https outside

iptables -A FORWARD -i eth0 -d 10.10.10.5 -p TCP --dport 80 -j ACCEPT

iptables -A FORWARD -i eth0 -d 10.10.10.5 -p TCP --dport 443 -j ACCEPT

#Allow return of http

iptables -A FORWARD -i eth1 -s 10.10.10.5 -p TCP --sport 80 -j ACCEPT

iptables -A FORWARD -i eth1 -s 10.10.10.5 -p TCP --sport 443 -j ACCEPT

#allow DNS in -> out

iptables -A FORWARD -i eth1 -p UDP --dport 53 -j ACCEPT

#allow dns return out -> inside

iptables -A FORWARD -i eth0 -p UDP --sport 53 -j ACCEPT

#ALLOW web browsing in -> out

```
iptables -A FORWARD -i eth1 -s 10.10.10.0/24 -p TCP --dport 80 -j ACCEPT
iptables -A FORWARD -i eth1 -s 10.10.10.0/24 -p TCP --dport 443 -j ACCEPT


#ALLOW web browsing out -> in
iptables -A FORWARD -i eth0 -d 10.10.10.0/24 -p TCP --sport 80 -j ACCEPT
iptables -A FORWARD -i eth0 -d 10.10.10.0/24 -p TCP --sport 443 -j ACCEPT

#Allow ICMP In->OUT
iptables -A FORWARD -i eth0 -p ICMP --icmp-type=0 -j ACCEPT
iptables -A FORWARD -i eth1 -p ICMP --icmp-type=8 -j ACCEPT

#Allow Mysql accessible from Warehouse

iptables -A FORWARD -i eth1 -p TCP -d 10.10.20.0/24 -s 10.10.10.0/24 --sport 3306 -j ACCEPT
iptables -A FORWARD -i eth0 -p TCP -d 10.10.10.0/24 -s 10.10.20.0/24 --dport 3306 -j ACCEPT


#ALLOW Access to webstore
#out->in
iptables -A FORWARD -i eth1 -d 10.10.20.0/24 -s 10.10.10.10 -p TCP --sport 80 -j ACCEPT
#in->out
iptables -A FORWARD -i eth0 -d 10.10.10.10 -s 10.10.20.0/24 -p TCP --dport 80 -j ACCEPT


#Allow internal dns
```

iptables -A FORWARD -i eth1 -d 10.10.20.0/24 -s 10.10.10.10 -p UDP --sport 53 -j ACCEPT

iptables -A FORWARD -i eth0 -d 10.10.10.10 -s 10.10.20.0/24 -p UDP --dport 53 -j ACCEPT

#Drop all packet coming from outside

iptables -A FORWARD -i eth0 -j DROP

#Drop all packet coming from inside

iptables -A FORWARD -i eth1 -j DROP