

Nftables

```
sudo su
apt install nftables
systemctl enable nftables.service && nft flush ruleset
nano /etc/nftables.conf
```

```
#!/usr/sbin/nft -f

flush ruleset

table ip filter {
    chain input {
        type filter hook input priority 0; policy drop;
        ct state related,established accept

        # Services
        ct state new tcp dport ssh counter accept
        ct state new tcp dport {80, 443} counter accept comment "HTTP"
        ct state new tcp dport 8000 counter accept comment "WEBMIN"

        # ICMP
        ip protocol icmp accept
        meta l4proto ipv6-icmp accept

        # Loopback
        iifname lo accept
    }

    chain forward {
        type filter hook forward priority 0; policy accept;
    }
}
```

```
chain output {  
    type filter hook output priority 0; policy accept;  
}  
}
```

```
nft -f /etc/nftables.conf  
nft list ruleset
```

```
#nft add rule ip filter input ct state new tcp dport 10050 counter accept comment "ZABBIX"
```

urls

<https://github.com/yoramvandevælde/nftables-example/blob/master/nftables-init.rules>

[nftables + Fail2Ban](#)

```
banaction = nftables-multiport  
banaction_allports = nftables-allports
```

From:
<https://ndp.pp.ua/> - my NoDeny Wiki

Permanent link:
<https://ndp.pp.ua/doku.php/debian/nftables?rev=1665530481>

Last update: **2022/10/11 23:21**

