```
/ip firewall filter

;;;retezec pro kontrolu tcp packetu
add chain=tcp_check protocol=tcp tcp-flags=syn, ack syn, ack \
connection-state=new action=reject reject-with=tcp-reset
add chain=tcp_check protocol=tcp tcp-flags=!syn connection-state=new \
action=log log-prefix="New not syn: "
add chain=tcp_check protocol=tcp tcp-flags=!syn connection-state=new action=drop

;;;retezec pro kontrolu povolenych packetu
add chain=allowed_packets protocol=tcp tcp-flags=syn action=accept
add chain=allowed_packets protocol=tcp connection-state=established action=accept
add chain=allowed_packets protocol=tcp connection-state=related action=accept
add chain=allowed_packets protocol=tcp action=drop

;;;retezec pro kontrolu icmp packetu
add chain=icmp_check protocol=icmp icmp-options=8:0 action=accept
add chain=icmp_check protocol=icmp icmp-options=11:0 action=accept


;;;INPUT

;;;vyhodime spatne tcp packety
add chain=input protocol=tcp action=jump jump-target=tcp_check

;;;vyhodime spatne icmp packety
add chain=input protocol=icmp in-interface=ether0 action=jump \
jump-target=icmp_check

;;;packety z DMZ interface
add chain=input in-interface=ether1 dst-address=192.168.1.1 action=accept

;;;packety z LAN interface
add chain=input in-interface=ether2 dst-address=192.168.2.1 action=accept

;;;DHCP requesty z LAN
add chain=input protocol=UDP in-interface=ether2 dst-port=67 src-port=68 \
action=accept

;;;povolime established a related spojeni z vnejsku
add chain=input dst-address=10.0.0.2 connection-state=established action=accept
add chain=input dst-address=10.0.0.2 connection-state=related action=accept

;;;zbyle nevyhovujici packety zalogujem a dropnem
add chain=input action=log log-prefix="INPUT dropped packet:"
add chain=input action=drop
```

```
;;;FORWARD

;;;vyhodime spatne packety
add chain=forward protocol=tcp action=jump jump-target=tcp_check

;;;packety z DMZ ven
add chain=forward in-interface=ether1 out-interface=ether0 action=accept

;;;navazana spojeni do DMZ
add chain=forward in-interface=ether0 out-interface=ether1 connection-
state=established action=accept
add chain=forward in-interface=ether0 out-interface=ether1 \
connection-state=related action=accept

;;;packety z LAN do DMZ
add chain=forward in-interface=ether2 out-interface=ether1 action=accept

;;;navazana spojeni z DMZ do LAN
add chain=forward in-interface=ether1 out-interface=ether2 connection-
state=established action=accept
add chain=forward in-interface=ether1 out-interface=ether2 \
connection-state=related action=accept

;;;HTTP server
add chain=forward protocol=TCP in-interface=ether0 out-interface=ether1 \
dst-address=192.168.1.2 dst-port=80 action=jump jump-target=allowed_packets
add chain=forward protocol=ICMP in-interface=ether0 out-interface=ether1 \
dst-address=192.168.1.2 dst-port=80 action=jump jump-target=icmp_check

;;;HTTPS
add chain=forward protocol=TCP in-interface=ether0 out-interface=ether1 \
dst-address=192.168.1.2 dst-port=443 action=jump jump-target=allowed_packets
add chain=forward protocol=ICMP in-interface=ether0 out-interface=ether1 \
dst-address=192.168.1.2 dst-port=443 action=jump jump-target=icmp_check

;;;SSH
add chain=forward protocol=TCP in-interface=ether0 out-interface=ether1 \
dst-address=192.168.1.2 dst-port=22 action=jump jump-target=allowed_packets
add chain=forward protocol=ICMP in-interface=ether0 out-interface=ether1 \
dst-address=192.168.1.2 dst-port=22 action=jump jump-target=icmp_check

;;;FTP
add chain=forward protocol=TCP in-interface=ether0 out-interface=ether1 \
dst-address=192.168.1.3 dst-port=21 action=jump jump-target=allowed_packets
add chain=forward protocol=ICMP in-interface=ether0 out-interface=ether1 \
dst-address=192.168.1.3 dst-port=21 action=jump jump-target=icmp_check
```

```
;;;packety z LAN
add chain=forward in-interface=ether2 action=accept

;;;navazana spojeni
add chain=forward connection-state=established action=accept
add chain=forward connection-state=related action=accept

;;;zbyle nevyhovujici packety zalogujem a dropnem
add chain=input action=log log-prefix="FORWARD dropped packet:"
add chain=input action=drop


;;;OUTPUT

;;;vyhodime spatne packety
add chain=output protocol=tcp action=jump jump-target=tcp_check

;;;packety z LAN a vnejsiho interface
add chain=output src-address=192.168.2.1 action=accept
add chain=output src-address=10.0.0.2 action=accept

;;;zbyle nevyhovujici packety zalogujem a dropnem
add chain=output action=log log-prefix="OUTPUT dropped packet:"
add chain=output action=drop


;;;DSTNAT

/ip firewall nat

;;;HTTP
add chain=dstnat dst-address=10.0.0.2 protocol=tcp dst-port=80 action=dst-nat \
to-addresses=192.168.1.2 to-ports=80

;;;HTTPS
add chain=dstnat dst-address=10.0.0.2 protocol=tcp dst-port=443 action=dst-nat \
to-addresses=192.168.1.2 to-ports=443

;;;FTP
add chain=dstnat dst-address=10.0.0.2 protocol=tcp dst-port=21 action=dst-nat \
to-addresses=192.168.1.3 to-ports=21

;;;SSH
add chain=dstnat dst-address=10.0.0.2 protocol=tcp dst-port=22 action=dst-nat \
to-addresses=192.168.1.2 to-ports=22

;;;tomcat
add chain=dstnat dst-address=10.0.0.2 protocol=tcp dst-port=8080 action=dst-nat \
to-addresses=192.168.1.2 to-ports=8080
```

```
;;;SRCNAT

add chain=srcnat out-interface=ether0 action=masquerade
```