

```
/ip firewall filter add chain=input protocol=tcp dst-port=21 src-address-list=ftp_blacklist action=drop comment="Drop FTP brute forcers" disabled=no

/ip firewall filter add chain=input protocol=tcp connection-state=established action=accept comment="Allow packets belonging to existing connections" disabled=no
/ip firewall filter add chain=input connection-state=related action=accept comment="Allow packets related to existing connections" disabled=no

/ip firewall filter add chain=input protocol=tcp dst-port=22 connection-state=new src-address-list=safe action=accept comment="Allow SSH safe hosts" disabled=no
/ip firewall filter add chain=input protocol=tcp dst-port=22 src-address-list=ssh_blacklist action=drop comment="Drop SSH brute forcers" disabled=no
/ip firewall filter add chain=input protocol=tcp dst-port=22 connection-state=new src-address-list=ssh_stage3 action=add-src-to-address-list address-list=ssh_blacklist address-list-timeout=10d comment="SSH brute forcers blacklisting" disabled=no
/ip firewall filter add chain=input protocol=tcp dst-port=22 connection-state=new src-address-list=ssh_stage2 action=add-src-to-address-list address-list=ssh_stage3 address-list-timeout=1m comment="SSH brute forcers the third stage" disabled=no
/ip firewall filter add chain=input protocol=tcp dst-port=22 connection-state=new src-address-list=ssh_stage1 action=add-src-to-address-list address-list=ssh_stage2 address-list-timeout=1m comment="SSH brute forcers the second stage" disabled=no
/ip firewall filter add chain=input protocol=tcp dst-port=22 connection-state=new action=add-src-to-address-list address-list=ssh_stage1 address-list-timeout=1m comment="SSH brute forcers the first stage" disabled=no

/ip firewall filter add chain=input protocol=tcp dst-port=8291 connection-state=new src-address-list=safe action=accept comment="Allow WinBox safe hosts" disabled=no
/ip firewall filter add chain=input protocol=tcp dst-port=8291 src-address-list=wb_blacklist action=drop comment="Drop WinBox brute forcers" disabled=no
/ip firewall filter add chain=input protocol=tcp dst-port=8291 connection-state=new src-address-list=wb_stage3 action=add-src-to-address-list address-list=wb_blacklist address-list-timeout=10d comment="WinBox brute forcers blacklisting" disabled=no
/ip firewall filter add chain=input protocol=tcp dst-port=8291 connection-state=new src-address-list=wb_stage2 action=add-src-to-address-list address-list=wb_stage3 address-list-timeout=1m comment="WinBox brute forcers the third stage" disabled=no
/ip firewall filter add chain=input protocol=tcp dst-port=8291 connection-state=new src-address-list=wb_stage1 action=add-src-to-address-list address-list=wb_stage2 address-list-timeout=1m comment="WinBox brute forcers the second stage" disabled=no
/ip firewall filter add chain=input protocol=tcp dst-port=8291 connection-state=new action=add-src-to-address-list address-list=wb_stage1 address-list-timeout=1m comment="WinBox brute forcers the first stage" disabled=no

/ip firewall filter add chain=input protocol=tcp dst-port=22 connection-state=new action=accept comment="Allow SSH" disabled=no
```

```
/ip firewall filter add chain=input protocol=tcp dst-port=8291 connection-state=new action=accept comment="Allow WinBox"
disabled=no
/ip firewall filter add chain=input protocol=tcp dst-port=20-21 connection-state=new action=accept comment="Allow FTP"
disabled=no

/ip firewall filter add chain=input protocol=tcp dst-port=1337 action=add-src-to-address-list address-list=knock address-
list-timeout=15s comment="Port knock-ing the first stage" disabled=no
/ip firewall filter add chain=input protocol=tcp dst-port=7331 src-address-list=knock action= add-src-to-address-list
address-list=safe address-list-timeout=15m comment="Port knocking whitelisting" disabled=no

/ip firewall filter add chain=input action=drop comment="Drop everything else"

/ip firewall filter add chain=output action=accept protocol=tcp content="530 Lo-gin incorrect" dst-limit=1/1m,9,dst-
address/1m comment="Allow only 10 FTP login incorrect answers per minute" disabled=no
/ip firewall filter add chain=output action=add-dst-to-address-list protocol=tcp content="530 Login incorrect" address-
list=ftp_blacklist address-list-timeout=3h comment="FTP brute forcers blacklisting" disabled=no
```