NTP Client Config:

```
/system ntp client
set enabled=yes primary-ntp=10.10.10.94
```

SNMP Config:

```
/snmp community
add authentication-password=AUTHPASS authentication-
protocol=SHA1 encryption-password=PRIVPASS encryption-
protocol=AES name=MYSNMP security=private
/snmp
set contact="NETSEC Lab" enabled=yes location=BD src-
address=10.10.10.11 trap-community=MYSNMP trap-generators=""
trap-interfaces=Mgmt_Do_Not_Delete trap-target=10.10.10.94
trap-version=3
```

Border Router IN Filter:

```
# BOGON List

/ip firewall address-list
add address=0.0.0.0/8 list=BOGON
add address=10.0.0.0/8 list=BOGON
add address=100.64.0.0/10 list=BOGON
add address=127.0.0.0/8 list=BOGON
add address=169.254.0.0/16 list=BOGON
add address=172.16.0.0/12 list=BOGON
add address=192.0.0.0/24 list=BOGON
add address=192.0.2.0/24 list=BOGON
add address=192.168.0.0/16 list=BOGON
add address=198.18.0.0/15 list=BOGON
add address=198.51.100.0/24 list=BOGON
add address=203.0.113.0/24 list=BOGON
add address=224.0.0.0/3 list=BOGON
add address=<your own prefix> list=BOGON

# IP Blacklists

/ip firewall address-list
add address=1.1.1.1/32 list=IP-BLACKLIST-IN


# DNS Whitelist

/ip firewall address-list
add address=2.2.2.2/32 list=DNS-ALLOW-IN

# SSH Whitelist

/ip firewall address-list
add address=2.2.2.2/32 list=SSH-ALLOW-IN
```

```
/ip firewall filter
add action=drop chain=forward in-interface=ether3 src-address-list=BOGON
comment="drop bogon sources"
add action=drop chain=forward in-interface=ether3 src-address-list=IP-
BLACKLIST-IN comment="drop bad sources"
add action=accept chain=forward in-interface=ether3 dst-address-list=DNS-
ALLOW-IN comment="accept DNS IN traffic"
add action=accept chain=forward in-interface=ether3 dst-address-list=SSH-
ALLOW-IN comment=" accept SSH IN traffic "



# TCP connection rules:

/ip firewall filter
add chain=forward protocol=tcp connection-state=invalid action=drop
comment="drop invalid connections"
add chain=forward connection-state=established action=accept comment="allow
already established connections"
add chain=forward connection-state=related action=accept comment="allow
related connections"


# Create Jump chain rules:

add chain=forward protocol=tcp action=jump jump-target=tcp
add chain=forward protocol=udp action=jump jump-target=udp
add chain=forward protocol=icmp action=jump jump-target=icmp

# TCP Rule:

add chain=tcp protocol=tcp dst-port=53 action=drop comment="deny DNS"
add chain=tcp protocol=tcp dst-port=69 action=drop comment="deny TFTP"
add chain=tcp protocol=tcp dst-port=111 action=drop comment="deny RPC
portmapper"
add chain=tcp protocol=tcp dst-port=135 action=drop comment="deny RPC
portmapper"
add chain=tcp protocol=tcp dst-port=137-139 action=drop comment="deny NBT"
add chain=tcp protocol=tcp dst-port=445 action=drop comment="deny cifs"
add chain=tcp protocol=tcp dst-port=2049 action=drop comment="deny NFS"
add chain=tcp protocol=tcp dst-port=12345-12346 action=drop comment="deny
NetBus"
add chain=tcp protocol=tcp dst-port=20034 action=drop comment="deny NetBus"
add chain=tcp protocol=tcp dst-port=3133 action=drop comment="deny
BackOriffice"
add chain=tcp protocol=tcp dst-port=67-68 action=drop comment="deny DHCP"

# UDP Rule:

add chain=udp protocol=udp dst-port=53 action=drop comment="deny DNS"
add chain=udp protocol=udp dst-port=69 action=drop comment="deny TFTP"
add chain=udp protocol=udp dst-port=111 action=drop comment="deny PRC
portmapper"
add chain=udp protocol=udp dst-port=123 action=drop comment="deny NTP"
add chain=udp protocol=udp dst-port=135 action=drop comment="deny PRC
portmapper"
add chain=udp protocol=udp dst-port=137-139 action=drop comment="deny NBT"
add chain=udp protocol=udp dst-port=161-162 action=drop comment="deny SNMP"
add chain=udp protocol=udp dst-port=2049 action=drop comment="deny NFS"
```

```
add chain=udp protocol=udp dst-port=3133 action=drop comment="deny
BackOriffice"

# ICMP Rule:

add chain=icmp protocol=icmp icmp-options=0:0 action=accept comment="echo
reply"
add chain=icmp protocol=icmp icmp-options=8:0 action=accept comment="allow
echo request"
add chain=icmp protocol=icmp action=drop comment="deny all other types"
```

Brute Force Login:

```
add chain=input protocol=tcp dst-port=22 src-address-list=ssh_blacklist
action=drop comment="drop ssh brute forcers" disabled=no

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="" disabled=no

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="" disabled=no

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="" disabled=no

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="" disabled=no

add chain=forward protocol=tcp dst-port=22 src-address-list=ssh_blacklist
action=drop comment="drop ssh brute downstream" disabled=no
```

Limit ICMP Packets:

```
/ip firewall mangle add action=mark-packet chain=prerouting new-packet-
mark=ICMP passthrough=yes protocol=icmp

/queue simple
add max-limit=1M/1M name=ICMP-BW-LIMIT packet-marks=ICMP target=0.0.0.0/0
```

TCP SYN FLOOD ATTACK:

```
/ip firewall filter add chain=input protocol=tcp connection-limit=LIMIT,32
action=add-src-to-address-list  address-list=blocked-addr address-list-
timeout=1d


/ip firewall filter add chain=input protocol=tcp src-address-list=blocked-
addr connection-limit=3,32 action=tarpit
```

```
/ip firewall filter add chain=forward protocol=tcp tcp-flags=syn
connection-state=new action=jump jump-target=SYN-Protect comment="SYN Flood
protect" disabled=yes
/ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn
limit=400,5 connection-state=new action=accept comment="" disabled=no
/ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn
connection-state=new action=drop comment="" disabled=no
```