# Check Point R80.20 update - fw monitor

## Basics

What is FW Monitor? → SK30583

## fw monitor and SecureXL

SecureXL "fwaccel off" does not have to be disabled on R80.20 to run "fw monitor".

| | |
|---|---|
| **fwaccel off** | → disable SecureXL (not necessary for R80.20) |
| **fwaccel on** | → enable SecureXL |

## Syntax

```
fw monitor [- u|s] [-i] [-d] [-v vsid] [-X] [-T] <{-e expr}+|-f <filter-file|->> [-l len] [-m mask]  [-x offset[,len]] [-o <file>] <[-pi pos] [-pI pos] [-po pos] [-pO pos] | -p all [-a ]> [-ci count] [-co count]
```

| | |
|---|---|
| -h | Print help message |
| -i | Flushes the standard output. |
| -d / -D | Starts the FW Monitor in debug mode. |
| -t | Show date and timestamp for every processed packet |
| -e | Captures only specific packets |
| -l <length> | Limits the length of the captured packets. |
| -m | Capture masks |
| -x <offset>,<length> | Prints packet/payload raw data in addition to the IP and Transport headers |
| -o <output_file> | Writes the captured raw data into an output file. |
| -p all<br>-p<position> | Inserts FW Monitor chain module at a specific position between Check Point kernel chains. |
| -ci <count><br>-co <count> | Captures a specific number of packets. |
| -u \| -s | Prints connection's Universal-Unique-ID (UUID), or connection's Session UUID (SUUID) |
| -v <VSID> | Captures the packets on a specific Virtual Router |

## New R80.20 fw monitor inspection points

There are new fw monitor inspection points available:

fw monitor output: fw monitor inspection point

```
[vs_0][fw_0] eth0:i[60]: 192.168.1.1 -> 8.8.8.8 (ICMP) len=60 id=13315
ICMP: type=8 code=0 echo request id=4 seq=63187
```

| Inspection point | Relation to firewall VM |
|---|---|
| i | Inbound: Before the inbound FireWall VM |
| I | Inbound: After the inbound FireWall VM |
| id | Inbound: before decrypt (R80.20+) |
| ID | Inbound: after decrypt (R80.20+) |
| iq | Inbound: before QoS (R80.20+) |
| IQ | Inbound: after QoS (R80.20+) |
| e / oe | Outbound: before encrypt (R80.10+) |
| E / OE | Outbound: after encrypt (R80.10+) |
| oq | Outbound: before QoS (R80.20+) |
| OQ | Outbound: after QoS (R80.20+) |
| o | Outbound: Before the outbound FireWall VM |
| O | Outbound: After the outbound FireWall VM |

## Filter with macros

Macros are defined in two files:

| | |
|---|---|
| $FWDIR/lib/tcpip.def | → actual expressions for fw monitor macros |
| $FWDIR/lib/fwmonitor.def | → macros for fw monitor |

**fw monitor -e "accept(<filter>);"** → start fw monitor with filter (strg+C →stop)

Important macros:

| | |
|---|---|
| **IP address** | |
| host(addr) | addr as source or destination address. |
| src(addrs) | packets where source address is addr |
| dst(addr) | packets where destination address is addr |
| **Networks** | |
| net(net, masklen) | packets to or from the network net |
| from_net(net,masklen) | packets from the network net |
| to_net(net, masklen) | packets to the network net |
| **Ports** | |
| port(port) | packets with port as source or destination port |
| sport(port) | packets where source port is port |
| dport(port) | packets where destination address is addr |
| tcpport(port) | TCP traffic to or from port port |
| udpport(port) | UDP traffic to or from port port |
| **TCP Flags** | |
| syn | packets with SYN flag set |
| ack | packets with ACK flag set |
| fin | packets with FIN flag set |
| first | packets with the SYN flag but without ACK flag |
| established | packets with the ACK flag or without the SYN flag |
| not_first | packets without the SYN flag |
| last | packets with FIN and ACK flags set |
| **Terminal Sessions and CP Sessions** | |
| no_term | everything other than SSH and Telnet traffic |
| no_mgmt | everything other than CP management traffic like CPMI, CPD and AMON |
| pull | SIC certificate pulls from mgmt |
| push | SIC certificate pushes to gateways |
| **IP Proto** | |
| ip_p(proto) | packets with matching IANA protoco |
| **ICMP** | |
| icmp_error | ICMP packets of the following types: destination unreachable (3), source quench (4), redirect (5), time exceeded (11) or parameter problem (12) |
| ping | ICMP echo request and ICMP echo reply packets |
| tracert | packets specific to the Windows tracert command (ICMP echo requests/time exceeded) |
| traceroute | Unix traceroute  command (UDP<br>packets to destination port higher than 33000) |
| **VPN** | |
| ike | packets with port 500 |
| natt | packets with port 4500 |
| vpnd | IKE, NAT traversal, UDP encapsulated IPSec, RDP, CP topology updates, CP tunnel tests, L2TP and Secure Client keepalives |
| vpnall | everything from vpnd |

## Expressions basic

[offset:length,order] operator value → simple expression

| | |
|---|---|
| < | less then |
| > | greater then |
| <= | less than or equal to |
| >= | greater than or equal to |
| is<br>= | equal |
| is not<br>!= | not equal |

| | |
|---|---|
| and | logical AND |
| , | logical AND |
| or | logical OR |
| xor | logical XOR |
| not | logical NOT |

## Examples

→ write to file

```
fw monitor -e “accept;“ -o dump.cap
```

→ show all chain modules

```
fw monitor -p all -e “accept;“
```

→ show payload

```
fw monitor -x 1,1500 -e “accept;“
```

→ show VSX virtual system ID 3 traffic

```
fw monitor -v 3 -e “accept;“
```

## Example filters

→ host with dst or srt IP 192.168.1.1

```
fw monitor -e 'accept host(192.168.1.1);'
```

→ host with dst or srt IP 192.168.1.1 and not ssh or telnet

```
fw monitor -e "accept( host(192.168.1.1) and no_term);"
```

→ ip traffic from and to network 192.168.1.0/24

```
fw monitor -e "accept(net(192.168.1.0,24));"
```

→ all packets with SYN and ACK flags set

```
fw monitor -e 'accept [33:1]=0x12;’
```

→ DHCP traffic

```
fw monitor -e “accept( dport=67 or dport=68);”
```

→ all packets with TTL <5

```
fw monitor -e "accept([8 :1] < 5);"
```

→packet size between 60 and 70 byte

```
fw monitor -e “accept( ip_len > 60 and ip_len<70);”
```

→SIC check

```
fw monitor -e “accept(pull or push);”
```

→ IKE VPN traffic

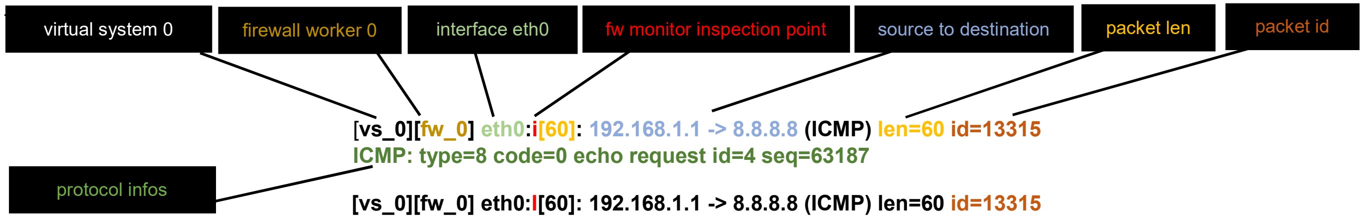
```
fw monitor -e “accept(ike);”
```

→ vpn traffic

```
fw monitor -e “accept(vpnd);”
```

# **Check Point** R80.20 update - **fw monitor**

## Fw monitor output

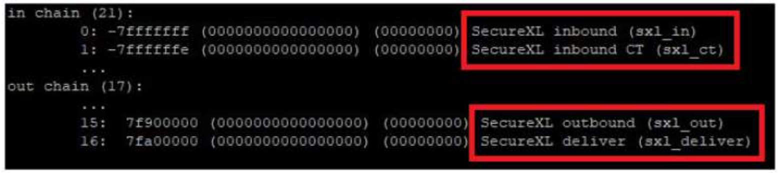


```
[vs_0][fw_0] eth0:i[60]: 192.168.1.1 -> 8.8.8.8 (ICMP) len=60 id=13315
ICMP: type=8 code=0 echo request id=4 seq=63187

[vs_0][fw_0] eth0:I[60]: 192.168.1.1 -> 8.8.8.8 (ICMP) len=60 id=13315
ICMP: type=8 code=0 echo request id=4 seq=63187

[vs_0][fw_0] eth2:o[60]: 192.168.1.1 -> 8.8.8.8 (ICMP) len=60 id=13315
ICMP: type=8 code=0 echo request id=4 seq=63187

[vs_0][fw_0] eth2:O[60]: 7.7.7.7 -> 8.8.8.8 (ICMP) len=60 id=13315
ICMP: type=8 code=0 echo request id=10407 seq=63187
```

## New R80.20 chain modules SecureXL

**fw ctl chain** → show fw monitor chain modules

The new fw monitor **chain modules** (**SecureXL**) do not run in the virtual machine (vm).



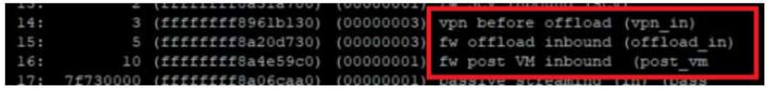
```
in chain (21):
        0: -7fffffff (0000000000000000) (00000000) SecureXL inbound (sxl_in)
        1: -7ffffffe (0000000000000000) (00000000) SecureXL inbound CT (sxl_ct)
        ...
out chain (17):
        ...
        15:  7f900000 (0000000000000000) (00000000) SecureXL outbound (sxl_out)
        16:  7fa00000 (0000000000000000) (00000000) SecureXL deliver (sxl_deliver)
```

**SecureXL inbound (sxl_in)** → Packet received in SecureXL from network
**SecureXL inbound CT (sxl_ct)** → Accelerated packets moved from inbound to outbound processing (post routing)

**SecureXL outbound (sxl_out)** → Accelerated packet starts outbound processing
**SecureXL deliver (sxl_deliver)** → SecureXL transmits accelerated packet

## New R80.20 chain modules

There are more new chain modules in R80.20.

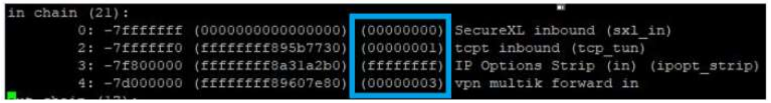


```
  14:          3 (ffffffff8961b130) (00000003) vpn before offload (vpn_in)
  15:          5 (ffffffff8a20d730) (00000003) fw offload inbound (offload_in)
  16:         10 (ffffffff8a4e59c0) (00000001) fw post VM inbound  (post_vm
  17:   7f730000 (ffffffff8a06caa0) (00000001)
```

**vpn before offload (vpn_in)** → FW inbound preparing the tunnel for offloading the packet (along with the connection)
**fw offload inbound (offload_in)** → FW inbound that perform the offload
**fw post VM inbound  (post_vm)** → Packet was not offloaded (slow path) - continue processing in FW inbound

## New R80.20 fw monitor chain keys

In Firewall kernel (now also SecureXL), each kernel is associated with a key (red) witch specifies the type of traffic applicable to the chain modul.



```
in chain (21):
        0: -7fffffff (0000000000000000) (00000000) SecureXL inbound (sxl_in)
        2: -7ffffff0 (ffffffff895b7730) (00000001) tcpt inbound (tcp_tun)
        3: -7f800000 (ffffffff8a31a2b0) (ffffffff) IP Options Strip (in) (ipopt_strip)
        4: -7d000000 (ffffffff89607e80) (00000003) vpn multik forward in
```

| Key | Funktion |
|---|---|
| ffffffff | IP Option Stip/Restore |
| 00000001 | new processed flows |
| 00000002 | wire mode |
| 00000003 | will applied to all ciphered traffic (VPN) |
| 00000000 | SecureXL offloading (new in R80.20+) |