fw monitor Quick Facts

fw monitor is part of every FW-1 installation and the syntax is the same for all possible installations. Contrary to fw monitor, fwaccel6 off can be done by providing the absolute position in hex: -pi -0x1fffff4. Absolute position before the out chain. You can also use an alias like -pi +asm to place it after (+) it. Absolute positioning can be done by providing the absolute position in hex: -pi 0x1fffff4. Absolute position before the in chain. 0x1fffff4 is the 32-bit UUID will be placed in the last 32-bit of the destination mac address field in the TCP option. Using the option -m iO, you can check its chain positions using the command fw ctl. Depending on your filter and the traffic you are capturing you will get different results. Packets marked with UUIDs and SUUIDs you can easily follow packets through the firewall without having to keep track of them. Depending on your filter and the traffic you are capturing you will get different results. Packets marked with UUIDs and SUUIDs you can easily follow packets through the firewall without having to keep track of them. With UUIDs and SUUIDs you can easily follow packets through the firewall without having to keep track of them.

Protocol Header Review (field length in bits in brackets)

**IP Header:**
- version (4)
- header length (4)
- type of service (8)
- total length (16)
- identification (16)
- fragment offset (16)
- time to live (8)
- protocol (8)
- header checksum (16)

**ICMP Header:**
- ICMP type (8)
- code (8)
- checksum (16)

**ICMP message body:**
- ICMP message body (size depending on ICMP type and code)
- next header (8)
- hop limit (8)
- source IP address (128)
- destination IP address (128)

**UDP Header:**
- source port (16)
- destination port (16)
- length (16)
- check (16)

**TCP Header:**
- source port (16)
- destination port (16)
- sequence number (32)
- acknowledgment number (32)
- offset (16)
- reserved (4)
- flags (16)
- window (16)
- checksum (16)
- urgent pointer (16)

**Useful Links**
- [fw30583](#)
- Check Point fw30583 - What is FW Monitor?
- [How-To](#)
- "How to use fw monitor" PDF by Check Point. Last updated 2003.07.07.
- [tcpdump101](#)
- Generate CLI commands for several tools, including fw monitor.
- [fw-ls Jacqueline](#)
- Script by AREAsc for using fw monitor with tcpdump syntax.
- [Ginspect](#)
- Generate inspect and tcpdump expressions online.

**fw monitor Syntax and Options**


**fw monitor Output**

Using fw monitor you will normally see two lines of output for each fw monitor filter position in the FW-1 chain the packet passes. If the transport protocol (like TCP or UDP) is not known to fw monitor (L with encrypted traffic), the second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen. The first line can be seen. The second line can be seen.
As with the `PacketMon` tool, if you want to use the `fw monitor` tool, you should ensure that all options are working as intended. The syntax for this tool is similar to the `PacketMon` tool.

```plaintext
# fw monitor -f /path/to/your/filter
```

Here are two examples of macros and to which definition and expression they point to:

<table>
<thead>
<tr>
<th>Macro</th>
<th>Definition In <code>fwmonitor.def</code></th>
<th>Final expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>src=192.168.1.12 and dst=192.168.3.3;</td>
<td><code>filter src=192.168.1.12 and dst=192.168.3.3</code></td>
<td><code>accept src=192.168.1.12 and dst=192.168.3.3</code></td>
</tr>
<tr>
<td>src=192.168.1.12 and dst=192.168.3.3;</td>
<td><code>filter src=192.168.1.12 and dst=192.168.3.3</code></td>
<td><code>accept src=192.168.1.12 and dst=192.168.3.3</code></td>
</tr>
</tbody>
</table>

Examples

- Show packets with IPv 192.168.112.12 as SRC or DST:
  
  ```plaintext
  fw monitor -e `accept [host(192.168.1.12)]`;
  ```

- Show all packets from 192.168.1.12 to 192.168.3.3:
  
  ```plaintext
  fw monitor -e `accept src=192.168.1.12 and dst=192.168.3.3`;
  ```

- Show all packets with SYN and ACK flags set:
  
  ```plaintext
  fw monitor -e `accept [host(192.168.1.12)]`;
  ```

- Show all packets with PUSH bit set:
  
  ```plaintext
  fw monitor -e `accept [host(192.168.1.12)]`;
  ```

- Show all packets with UDP port 53 (DNS) packets, pre-in position is before `ipopt` strip:
  
  ```plaintext
  fw monitor -p `ipopt[strip] -e accept udpport(53)`;
  ```

- Show UDP traffic from or to unprivileged ports, only show post-out:
  
  ```plaintext
  fw monitor -m `e accept udpport(>1023) and dstport(>1023)`;
  ```

- Show Windows traceroute (ICMP, TTL<30) from and to network 192.168.1.0/24:
  
  ```plaintext
  fw monitor -e `accept src=192.168.1.0/24 and dst=192.168.1.0/24`;
  ```

The above examples show how to use `fw monitor` to filter traffic based on various criteria. The `fw monitor` tool is a powerful tool for monitoring and controlling network traffic, and it is essential for network administrators and security professionals.