How To – Filter Packets using Packet Capture

Applicable to Version: 10.00 onwards

Packet capture displays packets details on the specified interface. It will provide connection details and details of the packets processed by each module packets e.g. firewall, IPS along with information like firewall rule number, user, Web and Application Filter policy number etc. This will help administrators to troubleshoot disruptive firewall rules.

Packet capture allows the user to intercept and display TCP/IP and other packets being transmitted or received over a network to which the device is attached.

The entire configuration is to be done from Web Admin Console. Access Web Admin Console with user having “Administrator” profile.

Filter Traffic using String Based Parameters

Go to System → Diagnostics → Packet Capture to capture information about packets. Click the “Configure” Button to configure filter settings for capturing the packets.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Bytes To Capture</td>
<td>Specify the number of bytes to be captured per packet.</td>
</tr>
<tr>
<td>(per packet)</td>
<td></td>
</tr>
<tr>
<td>Wrap Capture Buffer Once Full</td>
<td>Enable checkbox to continue capturing the packets even after the buffer is full.</td>
</tr>
<tr>
<td>Enter BPF String</td>
<td>host 172.16.16.18</td>
</tr>
<tr>
<td></td>
<td>Specify BPF string</td>
</tr>
<tr>
<td></td>
<td>BPF (Berkeley Packet Filter) sits between link-level driver and the user space. BPF is protocol independent and use a filter-before-buffering approach. It includes a machine abstraction to make the filtering efficient.</td>
</tr>
</tbody>
</table>
Click OK and to reflect the configuration changes, you need to stop and start the Packet Capture again.

**BPF String Parameters**

<table>
<thead>
<tr>
<th>How to check packets of the</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>specific host</td>
<td>host 10.10.10.1</td>
</tr>
<tr>
<td>specific source host</td>
<td>src host 10.10.10.1</td>
</tr>
<tr>
<td>specific destination host</td>
<td>dst host 10.10.10.1</td>
</tr>
<tr>
<td>specific network</td>
<td>net 10.10.10.0</td>
</tr>
<tr>
<td>specific source network</td>
<td>src net 10.10.10.0</td>
</tr>
<tr>
<td>specific destination network</td>
<td>dst net 10.10.10.0</td>
</tr>
<tr>
<td>specific port</td>
<td>Port 20 or port 21</td>
</tr>
<tr>
<td>specific source port</td>
<td>src port 21</td>
</tr>
<tr>
<td>specific destination port</td>
<td>dst port 21</td>
</tr>
<tr>
<td>specific host for the particular port</td>
<td>host 10.10.10.1 and port 21</td>
</tr>
<tr>
<td>the specific host for all the ports except SSH</td>
<td>host 10.10.10.1 and port not 22</td>
</tr>
<tr>
<td>specific protocol</td>
<td>proto ICMP, proto UDP, proto TCP or proto ARP</td>
</tr>
</tbody>
</table>

**Filter Traffic using Display Filter**

Display filter is used to filter captured traffic.

Go to **System → Diagnostics → Packet Capture** to capture information about packets. Click the “Display Filter” Button to specify the filter conditions for the packets.
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface Name</td>
<td>Select the physical interface from the list for filtering packets log.</td>
</tr>
<tr>
<td>Ether Type</td>
<td>IP</td>
</tr>
<tr>
<td></td>
<td>Select the Ethernet Type: IP or ARP.</td>
</tr>
<tr>
<td></td>
<td>EtherType is a field in an Ethernet frame. It is used to indicate the protocol encapsulated in the Ethernet frame.</td>
</tr>
<tr>
<td>Packet Type</td>
<td>TCP</td>
</tr>
<tr>
<td></td>
<td>Select the packet type used from the list for filtering packets.</td>
</tr>
<tr>
<td>Source IP</td>
<td>Specify Source IP Address of the Packet</td>
</tr>
<tr>
<td>Source Port</td>
<td>Specify Port Number</td>
</tr>
<tr>
<td>Destination IP</td>
<td>Specify Destination IP Address of the packet</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Specify Port Number</td>
</tr>
<tr>
<td>Reason</td>
<td>Reason for packet being dropped, if it is dropped</td>
</tr>
<tr>
<td>Status</td>
<td>Incoming: Packets received on on WAN or LAN interface.</td>
</tr>
<tr>
<td></td>
<td>Forwarded: Packet forwarded to Out Interface</td>
</tr>
<tr>
<td></td>
<td>Consumed: Packets designated for or used by the appliance</td>
</tr>
<tr>
<td></td>
<td>Generated: Packets generated by the appliance</td>
</tr>
<tr>
<td></td>
<td>Violation: In case of any policy violation, appliance will drop the packet and show the status “Violation”</td>
</tr>
<tr>
<td>Rule ID</td>
<td>Select specific firewall rule ID from where you want to sniff the network traffic.</td>
</tr>
<tr>
<td>User</td>
<td>Select Specific User or User Group on which you want to apply the filter</td>
</tr>
<tr>
<td>Connection ID</td>
<td>Connection ID can be retrieved from “Connection list” from System → Diagnostics → Connection list.</td>
</tr>
</tbody>
</table>
Click OK and the Display Filter will be applied successfully.

**Note:**

You can select any one or multiple parameters and can filter traffic based on the selected value.