Filter packets with Berkeley Packet Filter syntax

Published: 2024-11-01

Search for packets with the Berkeley Packet Filter (BPF) syntax alone, or in combination with the built-in filters.

Berkeley Packet Filters are a raw interface to data link layers and are a powerful tool for intrusion detection analysis. The BPF syntax enables users to write filters that quickly drill down on specific packets to see the essential information.

The ExtraHop system constructs a synthetic packet header from the packet index data and then runs the BPF syntax queries against the packet header to ensure that queries are much faster than scanning the full packet payload. Note that ExtraHop supports only a subset of the BPF syntax. See Supported BPF syntax.

The BPF syntax consists of one or more primitives preceded by one or more qualifiers. Primitives usually consist of an ID (name or number) preceded by one or more qualifiers. There are three different kinds of qualifiers:

type

Qualifiers that indicate what type the ID name or number refers to. For example, host, net, port, and portrange. If there is no qualifier, host is assumed.

dir

Qualifiers that specify a particular transfer direction to and or from an ID. Possible directions are src, dst, src and dst, and src or dst. For example, dst net 128.3.

proto

Qualifiers that restrict the match to the particular protocol. Possible protocols are ether, ip, ip6, tcp, and udp.

Add a filter with BPF syntax

- 1. Log in to the ExtraHop system through https://<extrahop-hostname-or-IP-address>.
- 2. From the top menu, click **Packets**.
- 3. In the trifield filter section, select **BPF**, and then type your filter syntax. For example, type src portrange 80-443 and net 10.10.
- 4. Click **Download PCAP** to save the packet capture with your filtered results.

- ExtraHop		Dashb	oards Ale	rts And	omalies	Metrics F	Records	Packets	Search	-			4	° 0	\$ ≜	DCTRDC 7207
C Last 30 minutes	•	Э	Packet Que	ries > N	New Packet	Query										
e Results		Packet	Query											45,483 g	ockets (47	92148)
v4														Dov	wnikoad PC	AP.
A138 (32.33M0)		From Feb	14, 2:40:56 pm									Until Feb 14, 3	10.56 pm			
10.9.30 (18.57MB)																
(10.9.27 (13.76M8)		BPF = s	rc portrange 80-	643 and net	10.10 ×											
the second se																
18.16.22 (6.76M0)		BPF ·					Add Filter	45,48	3 packets							
08.16.22 (6.76M8)).10.246.244 (6.76M8)		BPF	• • •				Add Filter	45,48	3 packets							
0.8.16.22 (6.76M8)).10.246.244 (6.76M8) \4.1.49 (5.36M8)		BPF	• • •				Add Filter Previewir	45,48 e 20 packet	3 packets s around Fe	6 14, 3:10:5	15.214 pm	•				
08.16.22 (6.76M8) 110.246.244 (6.76M8) 14.1.49 (5.36M8) 110.251.81 (2.00M8)		8PF	• • •	Sec 17	Þ	Dst IP	Add Filter Previewin	45,48 e 20 packet Sec Port	3 packets s around Fe Dist Port	6 14, 3 10 1 Flags	5.214 pm Bytes	Src MAC	Dist MAC		EtherType	VLAN ID
08.16.22 (6.7640) 1.10.246.244 (6.7648) 1.4.1.49 (5.3640) 1.10.251.81 (2.0048) 1.10.251.82 (8.39.3868) 1.10.251.82 (8.39.3868)		BPF	02-14 15:10:54	Sec 10	0.11.249	Dst IP 10.10.9.69	Add Filter Previewir IP Proto TCP	45,48 g 20 packet Sec Port 443	3 packets s around Fe Dist Port 4429	o 14, 3:10:1 Flags ACK	5.214 pm Bytes 66	Src MAC 44:A8:42:34:16:	Dit MAC 00:50:56:94:	2	EtherType IPv4	VLAN ID
08.16.22 (6.7640) 110.246.244 (6.7640) 14.1.49 (5.3640) 110.251.81 (2.0040) 110.251.82 (839.3840) 110.11.116 (792.0600) 110.251.179 (746.8403)		BPF 7	02-14 15:10:54	Sec II 	0.11.249 0.11.249	Dst IP 10.10.9.69 10.10.9.69	Add Filter Previewin IP Proto TCP TCP	45,48 e 20 packet Sec Port 443 443	3 packets s around Fe Dst Port 4429	ACK	5.214 pm Bytes 66 66	Src MAC 44.A8.42.34:16: 44.A8.42.34:16:	Dit MAC 00:50:56:943 00:50:56:943	12-	EtherType IPv4	VLAN ID
0.15.242 (6.7648) 0.10.246244 (6.7648) 0.41.49 (5.3640) 110.251.81 (2.0048) 110.251.81 (2.0048) 110.251.81 (2.0048) 110.251.179 (744.8488) 110.251.179 (744.8488) 110.245.211 (6.36.2380)		BPF 7	02-14 15:10:54.	Sec 8 10.1 10.1	0.11.249 0.11.249 0.11.249	Dat IP 10.10.9.69 10.10.9.69 10.10.252	Add Filter Previewin IP Proto TCP TCP	45,48 g 20 packet Set Port 443 443 443	3 packets s around Fe Dst Port 4429 4429	ACK	5.214 pm Bytes 66 66 27_	Src MAC 44.A8.42.34:16 44.A8.42.34:16 52.54:00:D8.21	Det MAC 00:50:56:943 00:50:56:943	12	EtherType IPv4 IPv4	VLAN ID

Supported BPF syntax

The ExtraHop system supports the following subset of the BPF syntax for filtering packets.

- **Note:** ExtraHop only supports numeric IP address searches. Hostnames are not allowed.
 - Indexing into headers, [...], is only supported for tcpflags and ip_offset. For example, tcp[tcpflags] & (tcp-syn|tcp-fin) != 0
 - ExtraHop supports both numeric and hexadecimal values for VLAN ID, EtherType, and IP Protocol fields. Prefix hexadecimal values with 0x, such as 0x11.

Primitive	Examples	Description			
[src dst] host <host ip=""></host>	host 203.0.113.50 dst host 198.51.100.200	Matches a host as the IP source, destination, or either. These host expressions can be specified in conjunction with other protocols like ip, arp, rarp or ip6.			
ether [src dst] host <mac></mac>	ether host 00:00:5E:00:53:00	Matches a host as the Ethernet source, destination, or either.			
	ether dst host 00:00:5E:00:53:00				
vlan <id></id>	vlan 100	Matches a VLAN. Valid ID numbers are 0–4095. VLAN priority bits are zero.			
		If the original packet had more than one VLAN tag, the synthetic packet the BPF matches against will only have the innermost VLAN tag.			
[src dst] portrange <pl>-</pl>	src portrange 80-88	Matches packets to or from a port			
<p2> or</p2>	tcp dst portrange 1501–1549	in the given range. Protocols can be applied to a port range to filter specific packets within the range.			
[tcp udp] [src dst] portrange <p1>-<p2></p2></p1>					
[ip ip6][src dst] proto	proto l	Matches IPv4 or IPv6 protocols other than TCP and UDP. The protocol can be a number or name.			
<protocol></protocol>	src 10.4.9.40 and proto ICMP				
	ip6 and src fe80::aebc:32ff:fe84:70b7 and proto 47				
	ip and src 10.4.9.40 and proto 0x0006				
[ip ip6][tcp udp] [src	udp and src port 2005	Matches IPv4 or IPv6 packets on a specific port.			
dst] port <port></port>	ip6 and tcp and src port 80				
[src dst] net <network></network>	dst net 192.168.1.0	Matches packets to or from a source or destination or either, that reside in a network. An IPv4 network number can be specified as one of the following values:			
	src net 10				
	net 192.168.1.0/24				
		• Dotted quad (x.x.x.x)			

Primitive	Examples	Description			
		 Dotted triple (x.x.x) Dotted pair (x.x) Single number (x) 			
[ip ip6] tcp tcpflags & (tcp-[ack fin syn rst	tcp[tcpflags] & (tcp- ack) !=0	Matches all packets with the specified TCP flag			
push urg)	tcp[13] & 16 !=0				
	ip6 and (ip6[40+13] & (tcp-syn) != 0)				
Fragmented IPv4 packets (ip_offset != 0)	ip[6:2] & 0x3fff != 0x0000	Matches all packets with fragments.			