Pakete mit der Berkeley-Paketfilter-Syntax filtern

Veröffentlicht: 2024-04-09

Suchen Sie nach Paketen mit der Berkeley Packet Filter (BPF) -Syntax allein oder in Kombination mit den integrierten Filtern.

Berkeley-Paketfilter sind eine einfache Schnittstelle zu Datenverbindungsebenen und ein leistungsstarkes Tool für die Analyse der Erkennung von Eindringlingen. Die BPF-Syntax ermöglicht es Benutzern, Filter zu schreiben, die schnell nach bestimmten Paketen suchen, um die wichtigsten Informationen zu sehen.

Das ExtraHop-System erstellt einen synthetischen Paket-Header aus den Paketindexdaten und führt dann die BPF-Syntaxabfragen für den Paket-Header aus, um sicherzustellen, dass Abfragen viel schneller sind als das Scannen der gesamten Paketnutzlast. Beachten Sie, dass ExtraHop nur eine Teilmenge der BPF-Syntax unterstützt. siehe Unterstützte BPF-Syntax.

Die BPF-Syntax besteht aus einem oder mehreren Primitiven, denen ein oder mehrere Qualifikatoren vorangestellt sind. Primitive bestehen normalerweise aus einer ID (Name oder Nummer), der ein oder mehrere Qualifikatoren vorangestellt sind. Es gibt drei verschiedene Arten von Qualifikationsspielen:

Art

Qualifikatoren, die angeben, auf welchen Typ sich der ID-Name oder die ID-Nummer bezieht. Zum Beispiel `host`, `net`, `port`, und `portrange`. Wenn es kein Qualifikationsmerkmal gibt, `host` wird angenommen.

dir

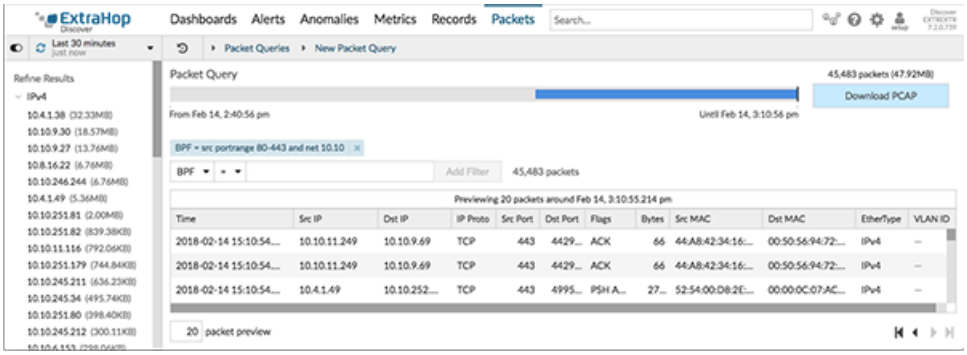
Qualifier, die eine bestimmte Übertragungsrichtung zu und/oder von einer ID angeben. Mögliche Richtungen sind `src`, `dst`, `src and dst`, und `src or dst`. Zum Beispiel `dst net 128.3`.

Proto

Qualifikatoren, die die Übereinstimmung auf das jeweilige Protokoll beschränken. Mögliche Protokolle sind `ether`, `ip`, `ip6`, `tcp`, und `udp`.

Fügen Sie einen Filter mit BPF-Syntax hinzu

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie im oberen Menü auf **Pakete**.
3. Wählen Sie im Bereich Dreifeld-Filter **BPF**, und geben Sie dann Ihre Filtersyntax ein. Geben Sie beispielsweise `src portrange 80-443 and net 10.10`.
4. klicken **PCAP herunterladen** um die PCAP mit Ihren gefilterten Ergebnissen zu speichern.



Unterstützte BPF-Syntax

Das ExtraHop-System unterstützt die folgende Teilmenge der BPF-Syntax zum Filtern von Paketen.

Hinweis
- ExtraHop unterstützt nur numerische IP-Adresssuchen. Hostnamen sind nicht erlaubt.
- Indizierung in Header, `[...]`, wird nur unterstützt für `tcpflags` und `ip_offset`. Zum Beispiel `tcp[tcpflags] & (tcp-syn|tcp-fin) != 0`
- ExtraHop unterstützt sowohl numerische als auch hexadezimale Werte für VLAN-ID-, EtherType- und IP-Protokollfelder. Stellen Sie Hexadezimalwerten 0x voran, z. B. 0x11.

Primitiv	Beispiele	Beschreibung
`[src|dst] host <host ip>`	`host 203.0.113.50` `dst host 198.51.100.200`	Entspricht einem Host als IP-Quelle, Ziel oder einer der beiden. Diese Host-Ausdrücke können in Verbindung mit anderen Protokollen wie ip, arp, rarp oder ip6 angegeben werden.
`ether [src|dst] host <MAC>`	`ether host 00:00:5E:00:53:00` `ether dst host 00:00:5E:00:53:00`	Entspricht einem Host als Ethernet-Quelle, Ziel oder einer der beiden.
`vlan <ID>`	`vlan 100`	Entspricht einem VLAN. Gültige ID-Nummern sind `0-4095`. Die VLAN-Prioritätsbits sind Null. Wenn das ursprüngliche Paket mehr als ein VLAN-Tag hatte, hat das synthetische Paket, mit dem der BPF übereinstimmt, nur das innerste VLAN-Tag.

`[src|dst] portrange <p1>-<p2>`
oder
`[tcp|udp] [src|dst] portrange <p1>-<p2>`
	`src portrange 80-88`
	`tcp dst portrange 1501-1549`
		Ordnet Pakete zu oder von einem Port im angegebenen Bereich zu. Protokolle können auf einen Portbereich angewendet werden, um bestimmte Pakete innerhalb des Bereichs zu filtern.

`[ip|ip6][src|dst] proto <protocol>`	`proto 1`
	`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`
		Entspricht anderen IPv4- oder IPv6-Protokollen als TCP und UDP. Das Protokoll kann eine Zahl oder ein Name sein.

`[ip|ip6][tcp|udp] [src|dst] port <port>`	`udp and src port 2005` `ip6 and tcp and src port 80`	Entspricht IPv4- oder IPv6-Paketen an einem bestimmten Port.

Primitiv	Beispiele	Beschreibung

`[src|dst] net <network>`	`dst net 192.168.1.0`
	`src net 10`
	`net 192.168.1.0/24`
		Ordnet Pakete zu oder von einer Quelle oder einem Ziel oder beidem zu, die sich in einem Netzwerk befinden. Eine IPv4-Netzwerknummer kann als einer der folgenden Werte angegeben werden:
		• Gepunktetes Viereck (x.x.x.x)
		• Dreifach gepunktet (x.x.x)
		• Gepunktetes Paar (x.x)
		• Einzelne Zahl (x)

`[ip|ip6] tcp tcpflags & (tcp-[ack|fin|syn|rst|push|urg|)`	`tcp[tcpflags] & (tcp-ack) !=0`
	`tcp[13] & 16 !=0`
	`ip6 and (ip6[40+13] & (tcp-syn) != 0)`
		Entspricht allen Paketen mit dem angegebenen TCP-Flag

Fragmentierte IPv4-Pakete (ip_offset! = 0)	`ip[6:2] & 0x3fff != 0x0000`	Stimmt mit allen Paketen mit Fragmenten überein.