Filtrer les paquets avec la syntaxe du filtre de paquets de Berkeley

Publié: 2023-09-19

Recherchez des paquets avec la syntaxe du filtre de paquets Berkeley (BPF), seule ou en combinaison avec les filtres intégrés.

Les filtres de paquets Berkeley sont une interface brute avec les couches de liaison de données et constituent un outil puissant pour l'analyse de la détection des intrusions. La syntaxe BPF permet aux utilisateurs d'écrire des filtres qui explorent rapidement des paquets spécifiques pour en extraire les informations essentielles.

Le système ExtraHop construit un en-tête de paquet synthétique à partir des données d'index des paquets, puis exécute les requêtes de la syntaxe BPF par rapport à l'en-tête du paquet afin de s'assurer que les requêtes sont beaucoup plus rapides que l'analyse de la charge utile complète du paquet. Notez qu'ExtraHop ne prend en charge qu'un sous-ensemble de la syntaxe BPF (voir Syntaxe BPF prise en charge).

La syntaxe BPF consiste en une ou plusieurs primitives précédées d'un ou plusieurs qualificatifs. Les primitives consistent généralement en un ID (nom ou numéro) précédé d'un ou plusieurs qualificatifs. Il existe trois types de qualificateurs :

le type

Qualificatifs indiquant à quel type le nom ou le numéro de l'identifiant se réfère. Par exemple, `host`, `net`, `port`, et `portrange`. En l'absence de qualificatif, `host` est considéré comme tel.

dir

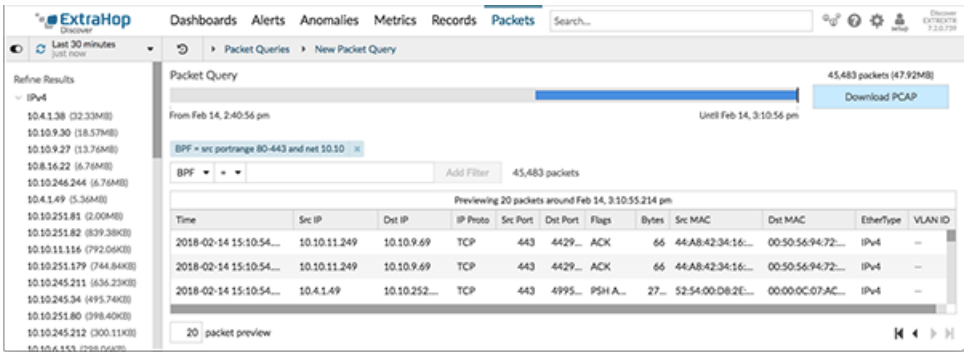
Qualificatifs indiquant une direction de transfert particulière vers ou à partir d'un ID. Les directions possibles sont `src`, `dst`, `src and dst`, et `src or dst`. Par exemple, `dst net 128.3`.

proto

Qualificatifs qui limitent la correspondance à un protocole particulier. Les protocoles possibles sont `ether`, `ip`, `ip6`, `tcp` et `udp`.

Ajouter un filtre avec la syntaxe BPF

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Dans le menu supérieur, cliquez sur **Paquets**.
3. Dans la section Filtre tri-champ, sélectionnez **BPF**, puis tapez la syntaxe de votre filtre. Par exemple, tapez `src portrange 80-443 and net 10.10`.
4. Cliquez sur **Télécharger PCAP** pour enregistrer la capture de paquets avec vos résultats filtrés.



Syntaxe BPF prise en charge

Le système ExtraHop prend en charge le sous-ensemble suivant de la syntaxe BPF pour le filtrage des paquets.

Note:
- ExtraHop ne prend en charge que les recherches numériques d'adresses IP. Les noms d'hôtes ne sont pas autorisés.
- L'indexation dans les en-têtes, `[...]`, n'est prise en charge que pour `tcpflags` et `ip_offset`. Par exemple, ExtraHop prend en charge à la fois les recherches numériques et les recherches dans les en-têtes, `tcp[tcpflags] & (tcp-syn|tcp-fin) != 0`
- ExtraHop prend en charge les valeurs numériques et hexadécimales pour les champs VLAN ID, EtherType et IP Protocol. Les valeurs hexadécimales sont préfixées par 0x, par exemple 0x11.

Primitive	Exemples de primitives	Description
`[src|dst] host <host ip>`	`host 203.0.113.50` `dst host 198.51.100.200`	Correspond à un hôte en tant que source IP, destination ou l'un ou l'autre. Ces expressions d'hôte peuvent être spécifiées en conjonction avec d'autres protocoles tels que ip, arp, rarp ou ip6.
`ether [src|dst] host <MAC>`	`ether host 00:00:5E:00:53:00` `ether dst host 00:00:5E:00:53:00`	Correspond à un hôte en tant que source Ethernet, destination ou l'un ou l'autre.
`vlan <ID>`	`vlan 100`	Correspond à un VLAN. Les numéros d'identification valides sont `0-4095`. Si le paquet d'origine avait plus d'une balise VLAN, le paquet synthétique auquel le BPF se réfère n'aura que la balise VLAN la plus interne .

`[src|dst] portrange <p1>-<p2>`
ou
`[tcp|udp] [src|dst] portrange <p1>-<p2>`
	`src portrange 80-88`
	`tcp dst portrange 1501-1549`
		Correspond aux paquets en provenance ou à destination d'un port dans la plage donnée. Les protocoles peuvent être appliqués à une plage de ports pour filtrer des paquets spécifiques dans cette plage.

`[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`
		Correspond aux protocoles IPv4 ou IPv6 autres que TCP et UDP. Le protocole peut être un numéro ou un nom.

Primitive	Exemples de primitives	Description
	`ip and src 10.4.9.40 and proto 0x0006`	
`[ip|ip6][tcp|udp] [src|dst] port <port>`	`udp and src port 2005` `ip6 and tcp and src port 80`	Correspond aux paquets IPv4 ou IPv6 sur un port spécifique.

`[src|dst] net <network>`	`dst net 192.168.1.0`
	`src net 10`
	`net 192.168.1.0/24`
		Correspond aux paquets en provenance ou à destination d'une source ou d'une destination, ou de l'une ou l'autre, qui résident dans un réseau. Un numéro de réseau IPv4 peut être spécifié comme l'une des valeurs suivantes :
		• quadruple pointillé (x.x.x.x)
		• Triple pointé (x.x.x)
		• Paire de points (x.x)
		• Nombre unique (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)`
		Correspond à tous les paquets avec l'indicateur TCP spécifié

Paquets IPv4 fragmentés (ip_offset != 0)	`ip[6:2] & 0x3fff != 0x0000`	Correspond à tous les paquets contenant des fragments.