

Paquets

Publié: 2023-12-05

Un paquet réseau est une petite quantité de données envoyée sur des réseaux TCP/IP (Transmission Control Protocol/Internet Protocol). Le système ExtraHop vous permet de collecter, de rechercher et de télécharger en permanence ces paquets à l'aide d'une appliance Trace, ce qui peut être utile pour détecter les intrusions sur le réseau et autres activités suspectes.

Vous pouvez rechercher et télécharger des paquets depuis la page Paquets du système ExtraHop et via le [Recherche par paquets](#) ressource dans l' API REST ExtraHop. Les paquets téléchargés peuvent ensuite être analysés par le biais d'un outil tiers, tel que Wireshark.

Note: Si vous ne possédez pas d'appliance Trace, vous pouvez toujours collecter des paquets via [déclencheurs](#). Voir [Initiez des captures de paquets de précision pour analyser les conditions de fenêtre zéro](#) à titre d'exemple.

Requête de paquets

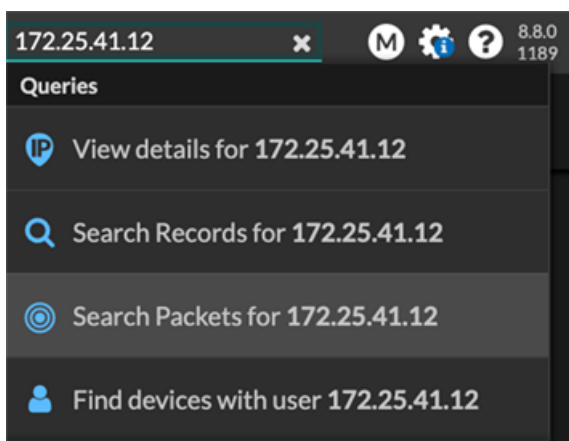
Lancez une requête rapide par paquet en cliquant sur **Paquets** depuis le menu supérieur. Le système ExtraHop interroge tous les paquets et affiche la page Packet Query. Si vous modifiez l'intervalle de temps, la requête recommence. Chaque extrémité de la barre grise affiche un horodateur, qui est déterminé par l'intervalle de temps actuel. L' heure sur la droite indique le point de départ de la requête et l'heure sur la gauche indique le point de terminaison de la requête. La barre bleue indique la plage de temps pendant laquelle le système a détecté des paquets. Vous pouvez faire glisser le pointeur pour zoomer sur une période dans la barre bleue afin de réexécuter une requête pendant l'intervalle de temps sélectionné.

La figure suivante fournit une vue d'ensemble de la page Packet Query et de ses fonctionnalités :

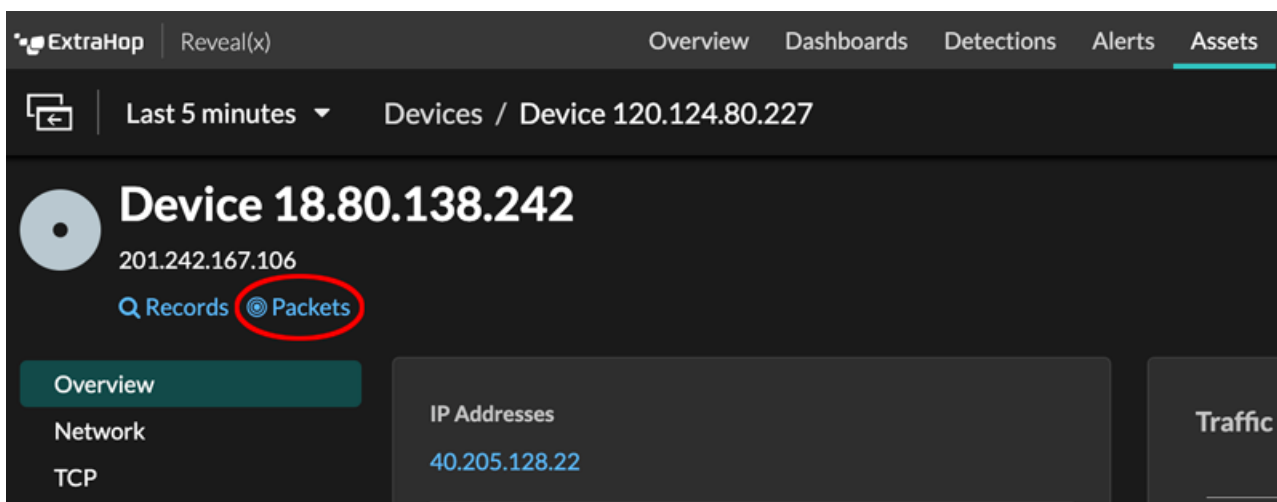
Conseil [Filtrer les paquets avec la syntaxe du filtre de paquets Berkeley](#).

Il existe plusieurs emplacements dans le système ExtraHop à partir desquels vous pouvez lancer une requête de paquet :

- Tapez une adresse IP dans le champ de recherche globale, puis sélectionnez l' icône Search Packets .



- Cliquez **Paquets** sur la page d'un équipement.



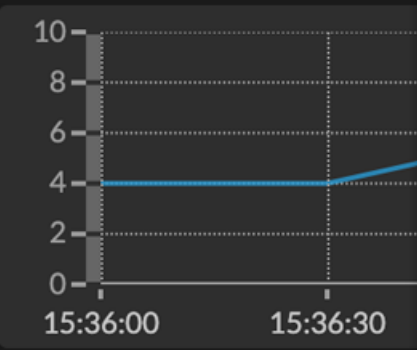
- Cliquez sur l'icône Packets à côté de n'importe quel enregistrement sur la page de résultats d'une requête d'enregistrement.

	Time ↓	Record Type
	2022-02-23 15:04:08.999	DNS Response
	2022-02-23 15:04:08.999	DNS Request
	2022-02-23 15:04:08.998	Flow
	2022-02-23 15:04:08.998	Flow
	2022-02-23 15:04:08.998	SSL Close

- Cliquez sur une adresse IP ou un nom d'hôte dans n'importe quel graphique contenant des métriques relatives aux octets ou aux paquets du réseau par adresse IP pour afficher un menu contextuel. Cliquez ensuite sur l'icône Packets pour demander l'équipement et l'intervalle de temps.

Overview Dashboards Detections Alerts Assets

Threat Hunting / HTTP



10
8
6
4
2
0

15:36:00 15:36:30

Any Field ≈

	Client IP
<input type="text"/>	100.152.8.59
<input type="text"/>	192.168.23.82

100.152.8.59
External Endpoint
Las Vegas, Nevada, United States

myip.opendns.com

Go To

- [ARIN Whois Lookup](#)
- [Records](#)
- [Packets](#)

[Go to IP Address Details](#)