Paquets

Publié: 2024-01-31

Un paquet réseau est une petite quantité de données envoyée sur les réseaux TCP/IP (Transmission Control Protocol/Internet Protocol). Le système ExtraHop vous permet de collecter, rechercher et 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 Recherche par paquets ressource dans l' API REST ExtraHop. Les paquets téléchargés peuvent ensuite être analysés via un outil tiers, tel que Wireshark.

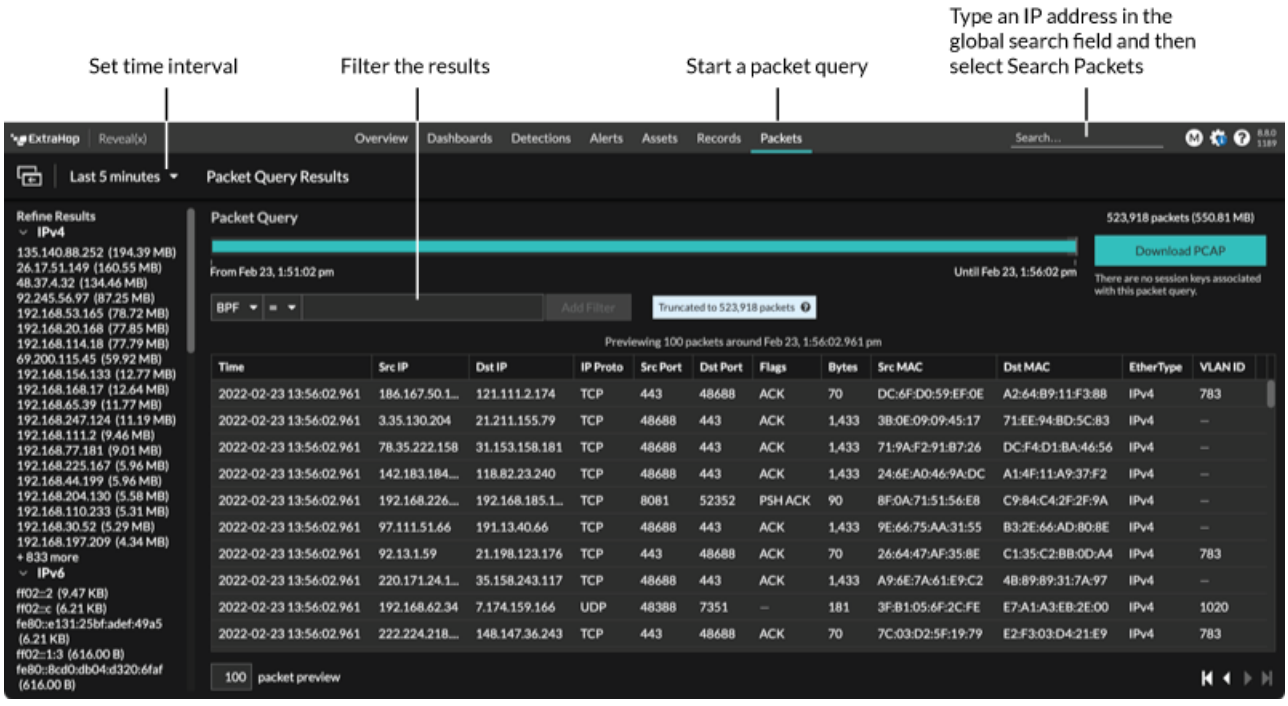
Note: Si vous ne possédez pas d'appliance Trace, vous pouvez toujours collecter des paquets via déclencheurs. Voir Initiez des captures de paquets de précision pour analyser les conditions de fenêtre zéro pour un exemple.

Vidéos Consultez la formation associée : Paquets

Requête de paquets

Lancez une requête rapide sur les paquets en cliquant **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 de droite indique le point de départ de la requête et l'heure de gauche indique le point de terminaison de la requête. La barre bleue indique l'intervalle de temps pendant lequel le système a détecté des paquets. Vous pouvez faire glisser le pointeur pour zoomer sur la barre bleue afin de lancer à nouveau une requête pour l'intervalle de temps sélectionné.

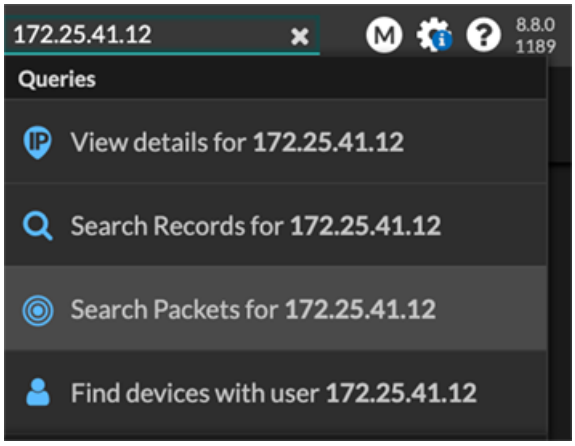
La figure suivante donne un aperçu de la page Packet Query et de ses fonctionnalités :



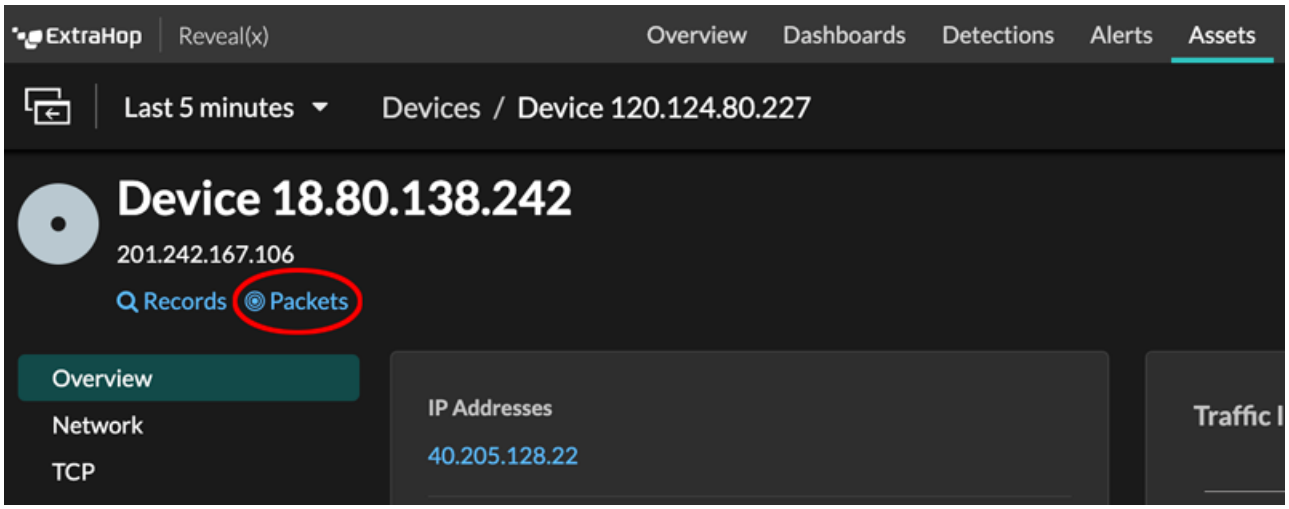
Conseil: Filtrer les paquets avec la syntaxe du filtre de paquets Berkeley.

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

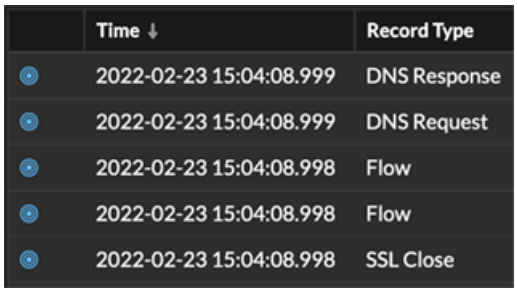
- Tapez une adresse IP dans le champ de recherche global, puis sélectionnez l' icône Rechercher des paquets .



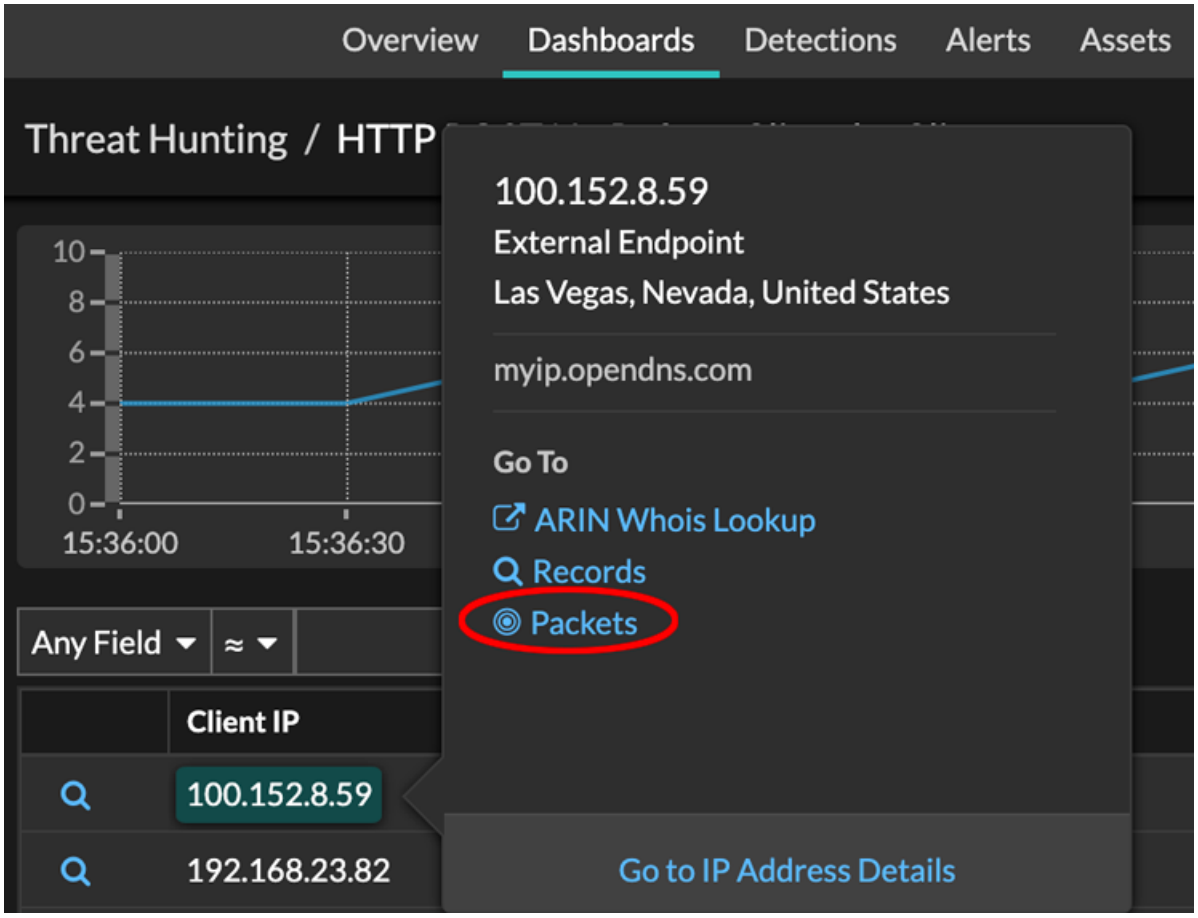
- Cliquez **Paquets** sur la page d'un équipement.



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



- Cliquez sur une adresse IP ou un nom d'hôte dans n'importe quel graphique contenant des mesures pour les octets du réseau ou les paquets par adresse IP pour afficher un menu contextuel. Cliquez ensuite sur l'icône Paquets pour rechercher 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
100.152.8.59
External Endpoint
Las Vegas, Nevada, United States
myip.opendns.com
Go To
ARIN Whois Lookup
Records
Packets
Any Field
≈
Client IP
100.152.8.59
192.168.23.82
Go to IP Address Details