Paquets

Publié: 2024-10-26

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.

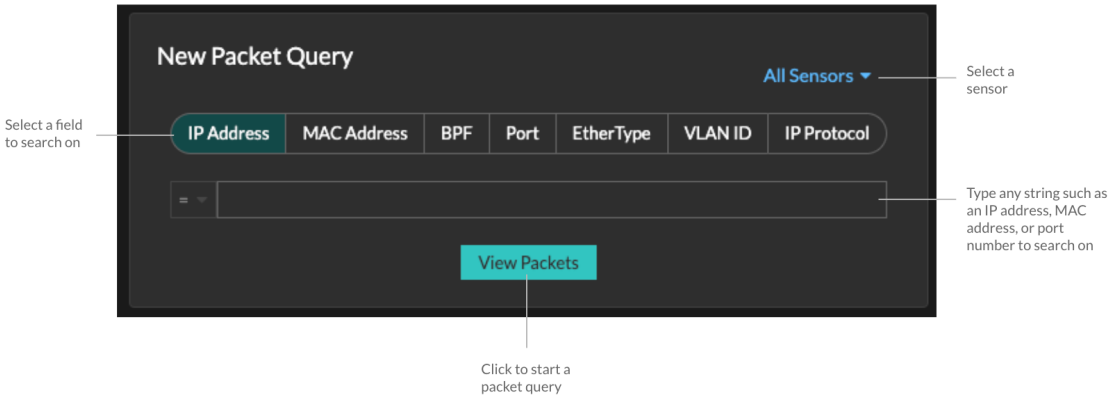
Vous pouvez rechercher et télécharger des paquets depuis la page Paquets du système ExtraHop et via Recherche par paquets ressource dans l' API REST ExtraHop. Les paquets téléchargés peuvent ensuite être analysés via un outil tiers, tel que Wireshark.

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.

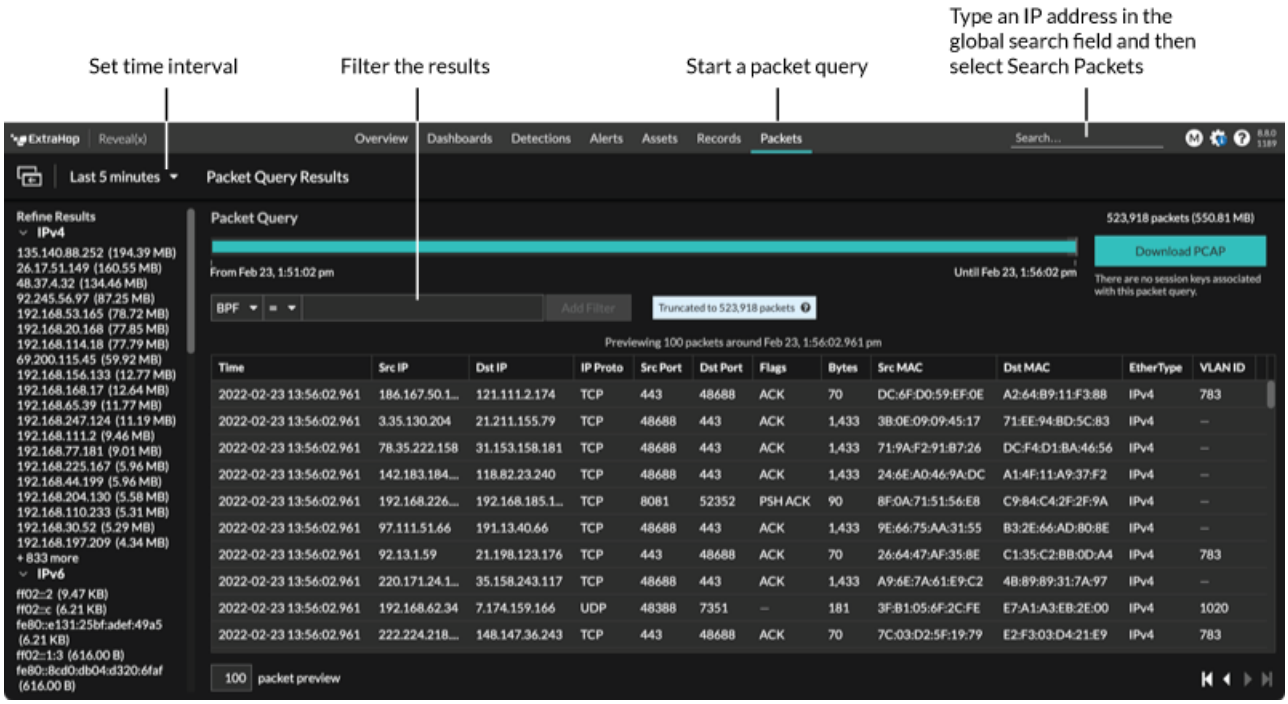
Vidéos Consultez la formation associée : Paquets

Navigation dans les paquets

Cliquez **Paquets** depuis le menu supérieur pour créer une nouvelle requête de paquet. Sur la page Nouvelle requête de paquet, vous pouvez spécifier un filtre.



Les résultats apparaissent sur la page principale Paquets page. Lancez une autre requête de paquet en cliquant sur **Paquets** à nouveau depuis le menu supérieur.



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 d'exécuter à nouveau une requête pour l'intervalle de temps sélectionné.

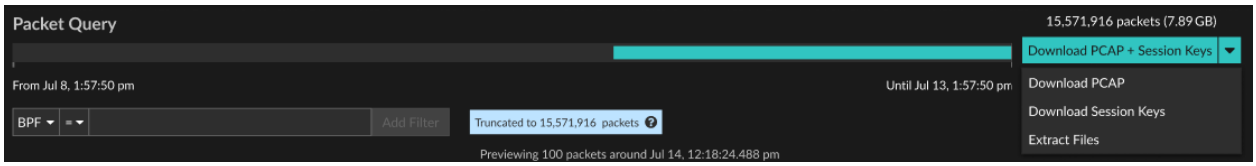
Conseil Filtrer les paquets avec la syntaxe du filtre de paquets Berkeley.

Note: Vous ne pouvez afficher que les paquets correspondant aux privilèges accordés par votre administrateur ExtraHop. Si les résultats de votre requête ne s'affichent pas, contactez votre administrateur ExtraHop.

Téléchargement de paquets

Vous pouvez télécharger les résultats des requêtes dans un fichier de capture de paquets (PCAP) à des fins d'analyse, ainsi que les clés de session TLS et les fichiers associés aux paquets.

Les options de téléchargement sont disponibles dans le menu déroulant en haut à droite. Cliquez sur une option pour permettre à votre navigateur de télécharger le fichier sur votre ordinateur local.



Voici quelques considérations concernant le téléchargement de paquets et l'extraction de fichiers :

- Les options de téléchargement affichées dans le menu déroulant dépendent des résultats de votre requête. Par exemple, si aucune clé de session n'est associée aux paquets, il se peut que seules les options de téléchargement du PCAP et d'extraction de fichiers s'affichent.
- Les téléchargements contiennent uniquement des paquets correspondant aux privilèges accordés par votre administrateur ExtraHop . Par exemple, si vous interrogez deux capteurs mais que votre

administrateur vous a attribué un accès limité à l'un des capteurs, votre téléchargement ne contiendra que les en-têtes de paquets provenant du capteur à accès limité.

- Si vous télécharger les clés de session, vous pouvez ouvrir le fichier de capture de paquets dans un outil tel que Wireshark, qui peut appliquer les clés de session et afficher les paquets déchiffrés.
- L'extraction de fichiers (également appelée découpage de fichiers) est disponible si des fichiers sont observés sur des paquets contenant des enregistrements HTTP ou SMB.

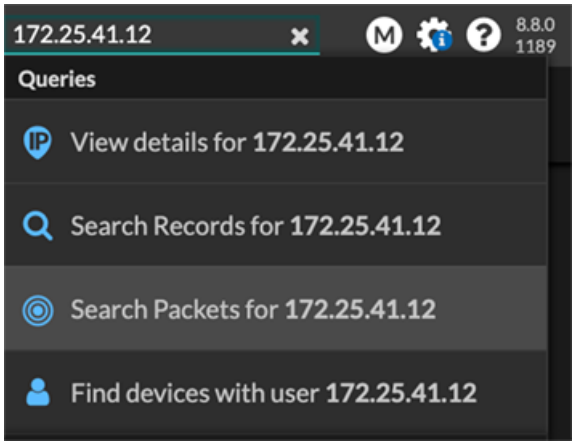
  Conseil: Sur la page Enregistrements, vous pouvez rechercher des types d'enregistrements HTTP ou SMB et filtrer par fichier observé. Cliquez sur l'icône des paquets à côté de l'enregistrement qui contient les fichiers que vous souhaitez extraire.
- Les fichiers extraits sont téléchargés dans un fichier .zip et contiennent un contenu original non chiffré susceptible d'inclure des données malveillantes. Un mot de passe est nécessaire pour ouvrir les fichiers .zip extraits. Le mot de passe est spécifié dans RevealX Enterprise ou RevealX 360 Les paramètres d'administration peuvent être obtenus auprès de votre administrateur ExtraHop.
- Si les options de téléchargement attendues ne s'affichent pas, contactez votre administrateur ExtraHop . Vous n'aurez aucun accès ou un accès limité aux capteurs qui ne vous sont pas attribués par le biais du contrôle d'accès aux capteurs. De plus, vos options de téléchargement peuvent être limitées par l'accès au module et les privilèges utilisateur. L'accès au module et les privilèges requis pour chaque option de téléchargement sont décrits dans le tableau suivant :

Option de téléchargement	Module requis	Privilèges Packet Forensics requis
Télécharger PCAP + Session Keys	NDR ou NPM	Paquets et clés de session
Télécharger PCAP	NDR ou NPM	Paquets uniquement
Télécharger PCAP Headers	NDR ou NPM	En-têtes de paquets uniquement
Télécharger PCAP Slices	NDR ou NPM	Tranches en sachets uniquement
Télécharger les clés de session	NDR ou NPM	Paquets et clés de session
Extraire des fichiers	NDR	Paquets uniquement ou Paquets et clés de session

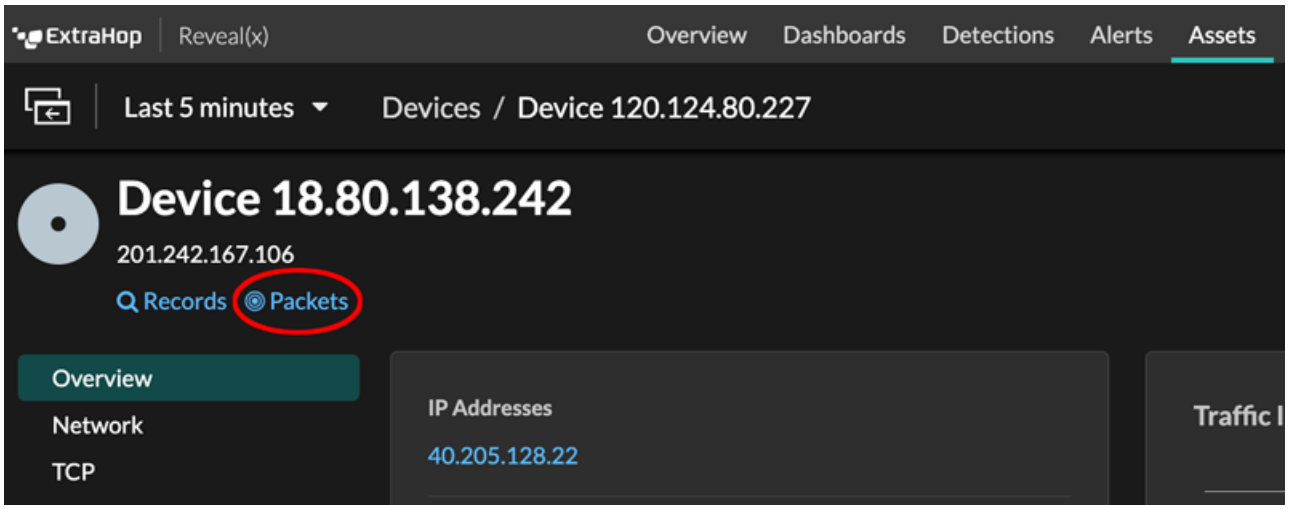
Paquets de requêtes dans le système ExtraHop

Bien que la page Paquets fournisse un accès rapide pour interroger tous les paquets, il existe des indicateurs et des liens à partir desquels vous pouvez lancer une requête de paquets dans le système ExtraHop.

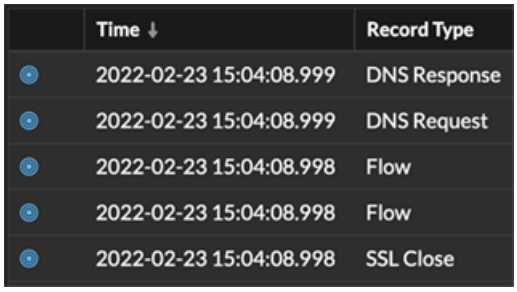
- Tapez une adresse IP dans le champ de recherche global, puis sélectionnez l' icône Rechercher des paquets .



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

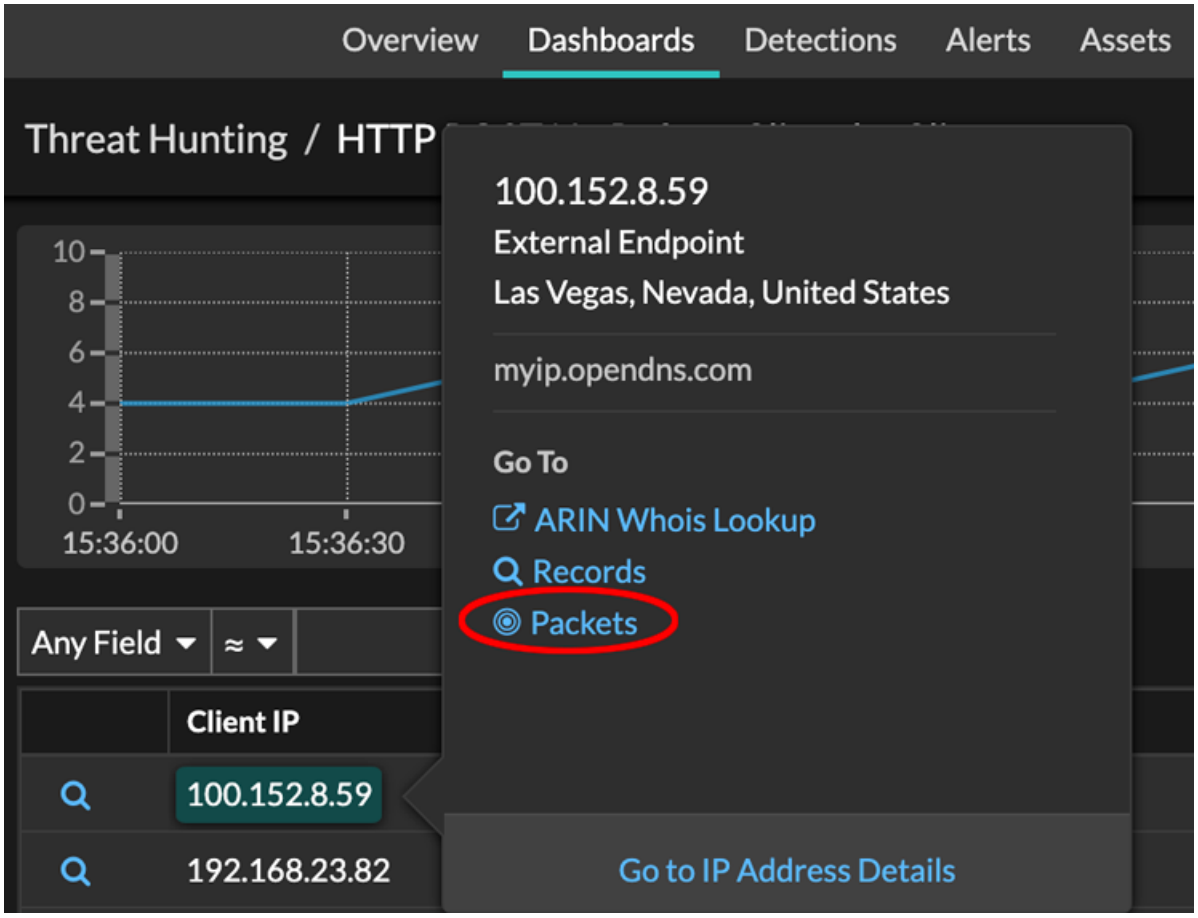


- Cliquez sur l'icône Paquets à côté de n'importe quel enregistrement sur la page de résultats d'une requête d'enregistrement.



	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 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
100.152.8.59
External Endpoint
Las Vegas, Nevada, United States
myip.opendns.com
Go To
ARIN Whois Lookup
Records
Packets
10
8
6
4
2
0
15:36:00
15:36:30
Any Field
≈
Client IP
100.152.8.59
192.168.23.82
Go to IP Address Details