

Paquets

Publié: 2024-08-09

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.

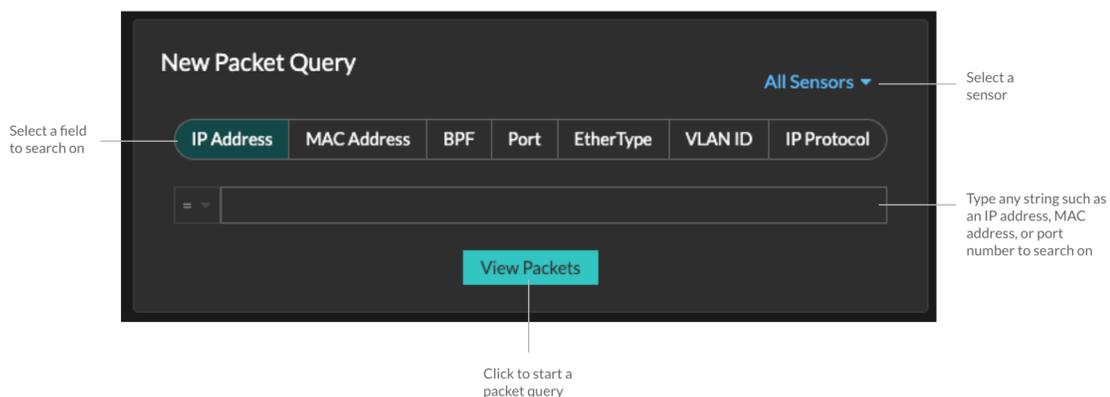
Vous pouvez rechercher et télécharger des paquets depuis la page Paquets du système ExtraHop et via [Recherche par paquets](#) ressource dans l' API REST ExtraHop. Les paquets téléchargés peuvent ensuite être analysés via un outil tiers, tel que Wireshark.

 **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.

 **Vidéo** 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 **Paquets** à nouveau depuis le menu supérieur.

Set time interval Filter the results Start a packet query Type an IP address in the global search field and then select Search Packets

Packet Query Results

Refine Results

- IPv4
 - 135.140.88.252 (194.39 MB)
 - 26.17.51.149 (160.55 MB)
 - 48.37.4.32 (134.46 MB)
 - 92.245.56.97 (87.25 MB)
 - 192.168.53.165 (78.72 MB)
 - 192.168.20.168 (77.85 MB)
 - 192.168.114.18 (77.79 MB)
 - 69.200.115.45 (69.92 MB)
 - 192.168.156.133 (12.77 MB)
 - 192.168.168.17 (12.64 MB)
 - 192.168.65.39 (11.77 MB)
 - 192.168.247.124 (11.19 MB)
 - 192.168.111.2 (9.46 MB)
 - 192.168.77.181 (9.01 MB)
 - 192.168.225.167 (5.96 MB)
 - 192.168.204.130 (5.58 MB)
 - 192.168.110.233 (5.31 MB)
 - 192.168.30.52 (5.29 MB)
 - 192.168.197.209 (4.34 MB)
 - + 833 more
- IPv6
 - ff02::2 (9.47 KB)
 - ff02::c (6.21 KB)
 - fe80::e131:25bf:adef:49a5 (6.21 KB)
 - ff02::1:3 (616.00 B)
 - fe80::8cd0:db04:d320:6faf (616.00 B)

Packet Query

523,918 packets (550.81 MB)

Download PCAP

From Feb 23, 1:51:02 pm Until Feb 23, 1:56:02 pm

BPF Add Filter Truncated to 523,918 packets

Previewing 100 packets around Feb 23, 1:56:02.961 pm

Time	Src IP	Dst IP	IP Proto	Src Port	Dst Port	Flags	Bytes	Src MAC	Dst MAC	EtherType	VLAN ID
2022-02-23 13:56:02.961	186.167.50.1...	121.111.2.174	TCP	443	48688	ACK	70	DC:6F:DD:59:EF:0E	A2:64:B9:11:F3:88	IPv4	783
2022-02-23 13:56:02.961	3.35.130.204	21.211.155.79	TCP	48688	443	ACK	1,433	3B:0E:09:09:A5:17	71:EE:94:8D:5C:83	IPv4	-
2022-02-23 13:56:02.961	78.35.222.158	31.153.158.181	TCP	48688	443	ACK	1,433	71:9A:F2:91:B7:26	DC:F4:D1:BA:46:56	IPv4	-
2022-02-23 13:56:02.961	142.183.184...	118.82.23.240	TCP	48688	443	ACK	1,433	24:6E:A0:46:9A:DC	A1:4F:11:A9:37:F2	IPv4	-
2022-02-23 13:56:02.961	192.168.226...	192.168.185.1...	TCP	8081	52352	PSH ACK	90	8F:0A:71:51:56:E8	C9:84:C4:2F:2F:9A	IPv4	-
2022-02-23 13:56:02.961	97.111.51.66	191.13.40.66	TCP	48688	443	ACK	1,433	9E:66:75:AA:31:55	B3:2E:66:AD:80:8E	IPv4	-
2022-02-23 13:56:02.961	92.13.1.59	21.198.123.176	TCP	443	48688	ACK	70	26:64:47:AF:35:BE	C1:35:C2:BB:0D:A4	IPv4	783
2022-02-23 13:56:02.961	220.171.24.1...	35.158.243.117	TCP	48688	443	ACK	1,433	A9:6E:7A:61:E9:C2	4B:89:89:31:7A:97	IPv4	-
2022-02-23 13:56:02.961	192.168.62.34	7.174.159.166	UDP	48388	7351	-	181	3F:B1:05:6F:2C:FE	E7:A1:A3:EB:2E:00	IPv4	1020
2022-02-23 13:56:02.961	222.224.218...	148.147.36.243	TCP	443	48688	ACK	70	7C:03:D2:5F:19:79	E2:F3:03:D4:21:E9	IPv4	783

100 packet preview

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 [🔗](#).

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 SSL 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.

Packet Query

15,571,916 packets (7.89 GB)

Download PCAP + Session Keys

From Jul 8, 1:57:50 pm Until Jul 13, 1:57:50 pm

BPF Add Filter Truncated to 15,571,916 packets

Download PCAP

Download Session Keys

Extract Files

Previewing 100 packets around Jul 14, 12:18:24.488 pm

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.
- 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 CIFS.



Conseil Sur la page Enregistrements, vous pouvez rechercher des types d'enregistrements HTTP ou CIFS et filtrer par fichier observé. Cliquez sur l'icône des paquets à côté de l'enregistrement qui contient les fichiers que vous souhaitez extraire.

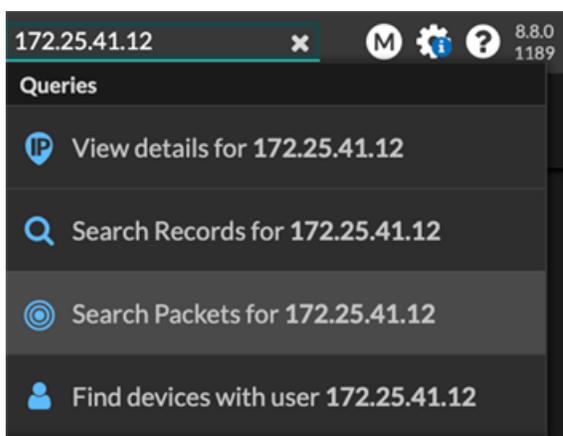
- Les fichiers extraits sont téléchargés dans un fichier .zip et contiennent un contenu original non chiffré susceptible d'inclure des données malveillantes.
- L'accès au module requis pour chaque option de téléchargement est décrit dans le tableau suivant :

Option de téléchargement	Module requis	Analyse des paquets requise
Télécharger PCAP + Session Keys	NDR ou NPM	Paquets et clés de session
Télécharger PCAP	NDR ou NPM	Paquets 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.

ExtraHop | Reveal(x) | Overview | Dashboards | Detections | Alerts | **Assets**

Last 5 minutes ▾ | Devices / Device 120.124.80.227

Device 18.80.138.242
201.242.167.106

Q Records **⊙ Packets**

Overview | Network | TCP

IP Addresses
40.205.128.22

Traffic I

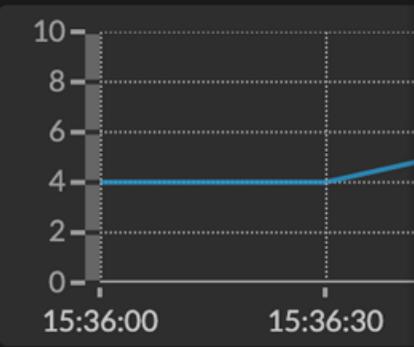
- Cliquez sur l'icône Paquets **⊙** à côté de n'importe quel enregistrement sur la page de résultats d'une requête d'enregistrement.

	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



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](#)