


Paquets

Publié: 2024-04-10

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.

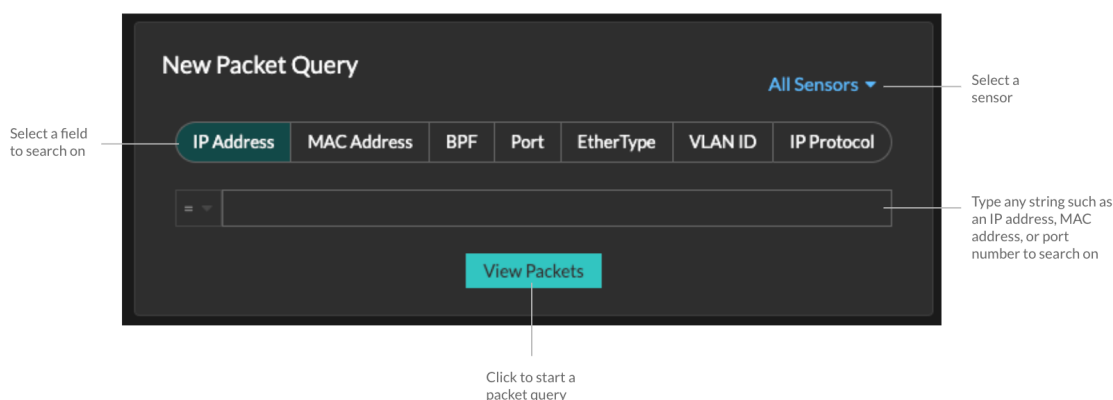
Vous pouvez rechercher et télécharger des paquets depuis la page Paquets du système ExtraHop et via [Recherche par paquets](#) ressource dans l' API REST ExtraHop. Les paquets téléchargés peuvent ensuite être analysés via un outil tiers, tel que Wireshark.

 **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


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:00:59: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:09:09:45:17	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

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.



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.

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 | IP Addresses | Traffic I

Network | 40.205.128.22

TCP

- 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
100.152.8.59
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