VPN-Erkennung

Veröffentlicht: 2024-02-16

VPN Discovery ermöglicht es dem ExtraHop-System, die privaten RFC-1918-IP-Adressen, die VPN-Clients zugewiesen wurden, mit ihren öffentlichen, externen IP-Adressen zu korrelieren. Dieser verbesserte Einblick in den Nord-Süd-Verkehr reduziert Barrieren bei der Untersuchung von Sicherheitsvorfällen und Leistungsproblemen, an denen externe VPN-Clients beteiligt sind.

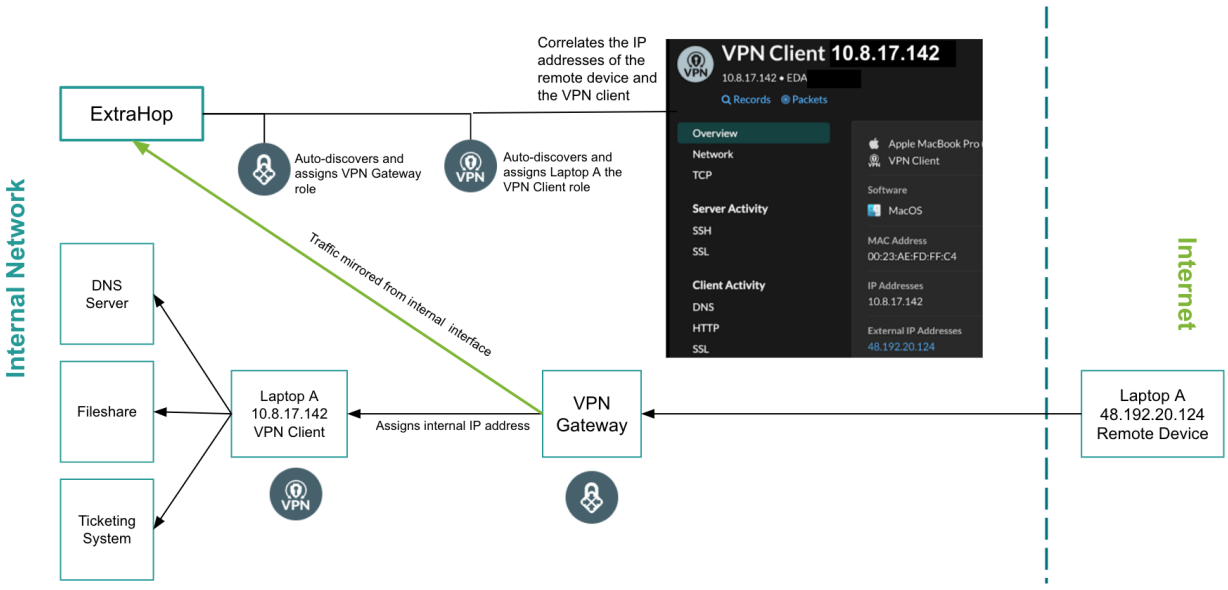
Der ExtraHop Machine Learning Service aggregiert WAN-seitige Geräte mit aktiven Tunneln zu einem VPN-Gateway, analysiert den Datenverkehr von beiden Seiten des VPN-Gateways und erkennt und klassifiziert diese Geräte dann automatisch als VPN-Clients. Sie können dann die externen und internen IP-Adressen für Geräte sehen, denen die VPN-Client-Rolle zugewiesen ist, und Sie können die Verlauf für alle IP-Adressen wird vom System erkannt, sodass Sie verfolgen können, wann sich eine IP-Adresse für einen Benutzer ändert.

Die folgenden Systemanforderungen müssen für VPN Discovery erfüllt sein:

- Das ExtraHop-System muss verbunden mit ExtraHop Cloud Services weil VPN Discovery den Machine Learning Service benötigt.
- Das ExtraHop-System muss aktiviert für VPN Client Discovery.
- Das ExtraHop-System muss Einblick in die internen und externen Schnittstellen des VPN-Gateways haben.

VPN Discovery kann nur funktionieren, wenn das ExtraHop-System Zugriff auf beide Seiten (oder Schnittstellen) des VPN-Gateways hat. Bei den meisten VPN-Gateways und in einarmigen Konfigurationen kann das ExtraHop-System die VPN-Gateway-Rolle automatisch erkennen und Geräten in Ihrem Netzwerk zuweisen, die VPN-Verbindungen empfangen. Aktivieren Sie die automatische Klassifizierung und Zuweisung der VPN-Gateway-Rolle in der laufenden Konfigurationsdatei. Wenn Ihr VPN-Gateway nicht vom System klassifiziert wird, müssen Sie die VPN-Gateway-Rolle manuell zuweisen.

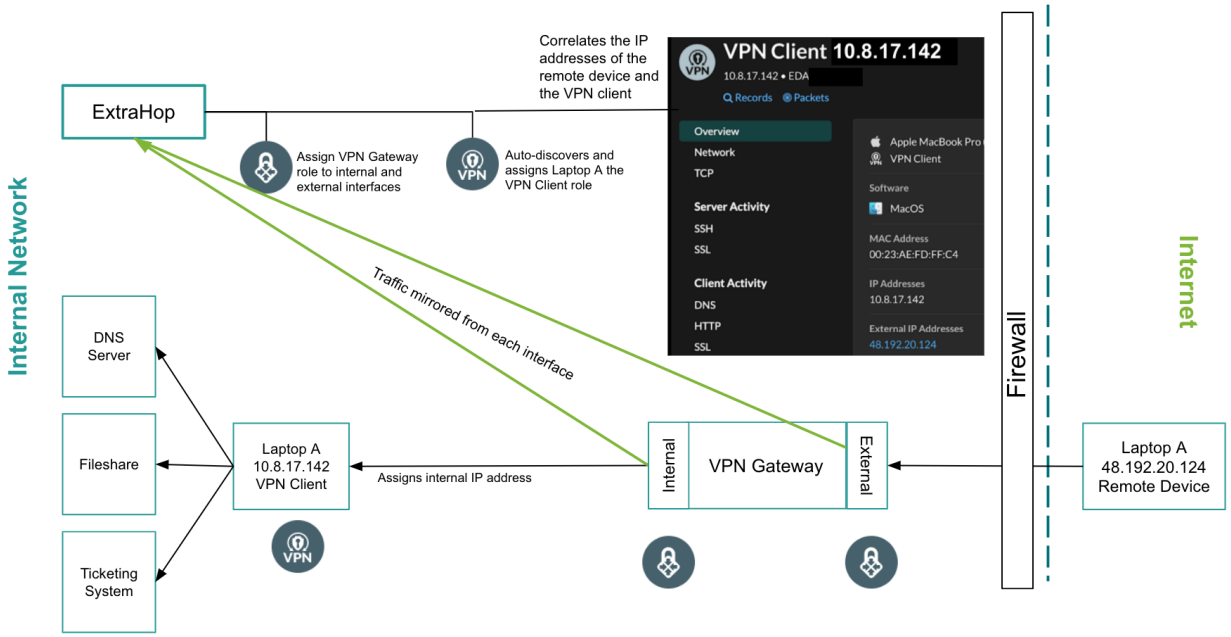
Wenn das System die VPN-Gateway-Rolle einem Router zuweist, der einen Teil des VPN-Verkehrs verarbeitet, ändern Sie die Geräterolle für den Router manuell in die Gateway-Rolle und weisen Sie die VPN-Gateway-Rolle dem richtigen Gerät in Ihrem Netzwerk zu.



Die VPN-Client-Geräterolle wird vom System nur Geräten mit einer RFC-1918-IP-Adresse (oder einer privaten) IP-Adresse zugewiesen. Diese Geräte werden automatisch klassifiziert, wenn sie als Kind eines VPN-Gateways erkannt werden. Die VPN-Client-Rolle kann nicht manuell zugewiesen werden.

Zweiarmige Konfigurationen

Bei VPN-Gateways, die in zweiarmigen Konfigurationen eingesetzt werden, müssen Sie die VPN-Gateway-Rolle manuell der internen Schnittstelle des VPN-Gateways zuweisen. Nur die externe Schnittstelle wird vom ExtraHop-System automatisch klassifiziert.



Nachdem die VPN-Gateway-Rollen den internen und externen Schnittstellen zugewiesen wurden, erkennt das ExtraHop-System automatisch VPN-Client-Geräte für alle RFC-1918-IP-Adressen (oder privaten IP-Adressen), die über das VPN-Gateway zugewiesen wurden.

L2 und L3 Discovery

VPN Discovery funktioniert, wenn das ExtraHop-System für eines der beiden konfiguriert ist L2 Discovery oder L3 Discovery.

- In L2 Discovery werden VPN-Gateways immer als L2-Geräte klassifiziert und haben einen einzigen Geräteeintrag im System.
- In L3 Discovery wird sowohl dem untergeordneten L3-Eintrag als auch dem übergeordneten L2-Eintrag für das VPN-Gateway die VPN-Gateway-Rolle zugewiesen.

Segmentierte VPN-Gateways

Wenn Ihr VPN-Gateway so segmentiert ist, dass der Datenverkehr nicht von beiden Schnittstellen gespiegelt werden kann, können Sie Sammeln Sie Beobachtungen über die ExtraHop REST API und verknüpfen Sie internen und externen Verkehr manuell.