Découverte d'un VPN

Publié: 2024-08-08

VPN Discovery permet au système ExtraHop de corréler les adresses IP privées de la RFC-1918 attribuées aux clients VPN avec leurs adresses IP publiques externes. Cette visibilité accrue sur le trafic nord-sud réduit les obstacles lors des enquêtes sur les incidents de sécurité et les problèmes de performance impliquant des clients VPN externes.

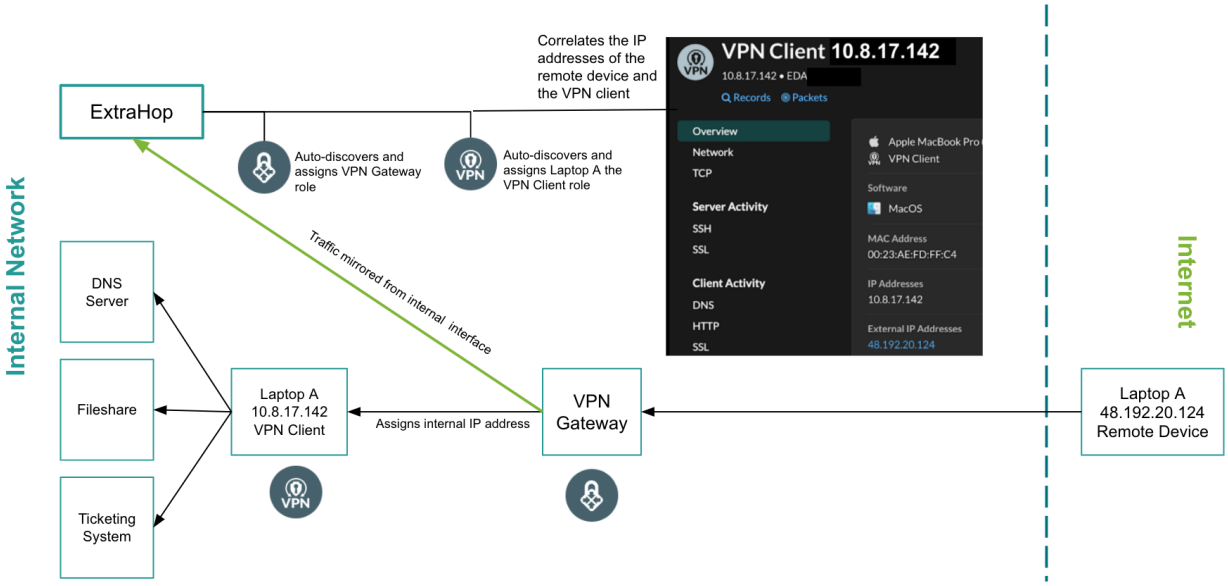
Le service d'apprentissage automatique ExtraHop regroupe les appareils côté WAN dotés de tunnels actifs vers une passerelle VPN, analyse le trafic provenant des deux côtés de la passerelle VPN, puis découvre et classe automatiquement ces appareils en tant que clients VPN. Vous pouvez ensuite voir les adresses IP externes et internes des appareils auxquels le rôle de client VPN a été attribué, et vous pouvez voir historique de toutes les adresses IP découvert par le système afin que vous puissiez suivre le changement d'adresse IP d'un utilisateur.

La configuration système requise suivante doit être respectée pour VPN Discovery :

- Le système ExtraHop doit être connecté aux services cloud ExtraHop car VPN Discovery nécessite le service d'apprentissage automatique.
- Le système ExtraHop doit être activé pour VPN Client Discovery.
- Le système ExtraHop doit avoir une visibilité sur les interfaces internes et externes de la passerelle VPN.

VPN Discovery ne peut fonctionner que lorsque le système ExtraHop a accès aux deux côtés (ou interfaces) de la passerelle VPN. Pour la plupart des passerelles VPN et dans les configurations à bras unique, le système ExtraHop peut détecter et attribuer automatiquement le rôle de passerelle VPN aux appareils de votre réseau qui reçoivent des connexions VPN. Activez la classification et l' attribution automatiques du rôle de passerelle VPN dans le fichier de configuration en cours d'exécution. Si votre passerelle VPN n'est pas classée par le système, vous devez attribuer manuellement le rôle de passerelle VPN.

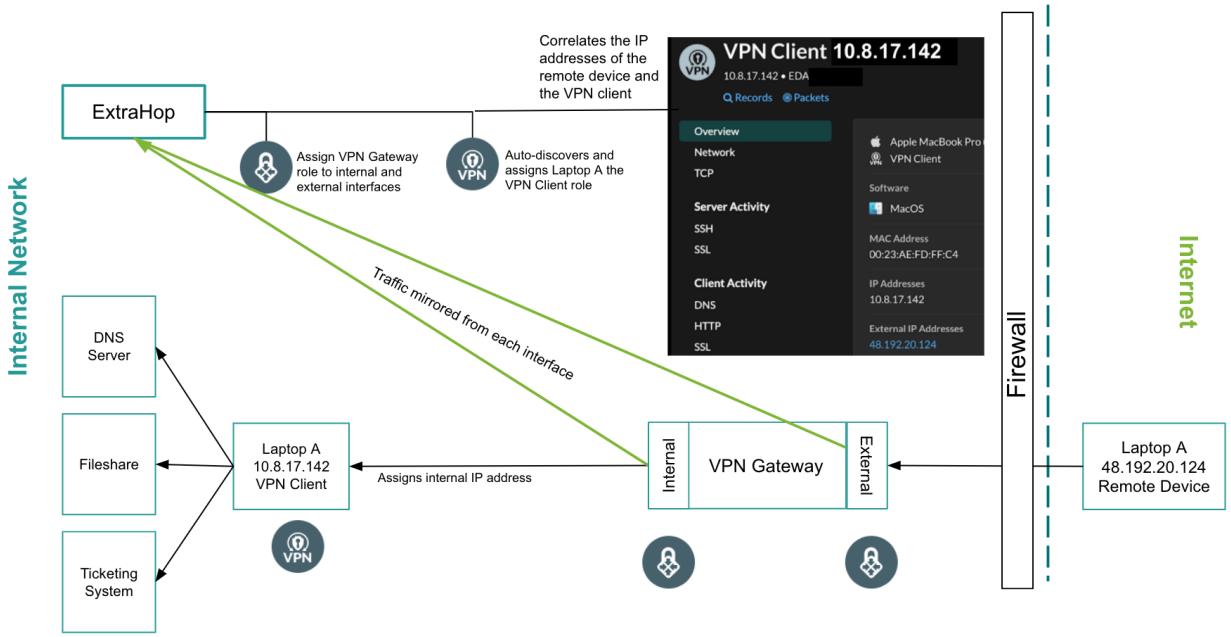
Si le système attribue le rôle de passerelle VPN à un routeur qui gère une partie du trafic VPN, remplacez manuellement le rôle d'équipement du routeur par le rôle de passerelle et attribuez le rôle de passerelle VPN au bon équipement de votre réseau.



Le rôle d'équipement client VPN est uniquement attribué par le système aux appareils dotés d'une adresse IP RFC-1918 (ou privée). Ces appareils sont automatiquement classés lorsqu'ils sont découverts en tant qu'enfants d'une passerelle VPN. Le rôle de client VPN ne peut pas être attribué manuellement.

Configurations à deux bras

Pour les passerelles VPN déployées dans des configurations à deux bras, vous devez attribuer manuellement le rôle de passerelle VPN à l'interface interne de la passerelle VPN ; seule l'interface externe est automatiquement classée par le système ExtraHop.



Une fois les rôles de passerelle VPN attribués aux interfaces internes et externes, le système ExtraHop découvre automatiquement les périphériques clients VPN pour toutes les adresses IP RFC-1918 (ou privées) attribuées via la passerelle VPN.

L2 et L3 Discovery

VPN Discovery fonctionne lorsque le système ExtraHop est configuré pour L2 Discovery ou L3 Discovery.

- Dans L2 Discovery, les passerelles VPN sont toujours classées comme des appareils L2 et ne comportent qu'une seule entrée d'équipement dans le système.
- Dans L3 Discovery, le rôle de passerelle VPN est attribué à l'entrée enfant L3 et à l'entrée parent L2 de la passerelle VPN.

Passerelles VPN segmentées

Si votre passerelle VPN est segmentée de manière à empêcher le trafic d'être reflété depuis les deux interfaces, vous pouvez collecter des observations via l'API REST ExtraHop et associez manuellement le trafic interne au trafic externe.