VPN Discovery

Published: 2023-11-15

VPN Discovery enables the ExtraHop system to correlate the private, RFC-1918 IP addresses assigned to VPN clients with their public, external IP addresses. This enriched visibility into north-south traffic reduces barriers when investigating security incidents and performance issues that involve external VPN clients.

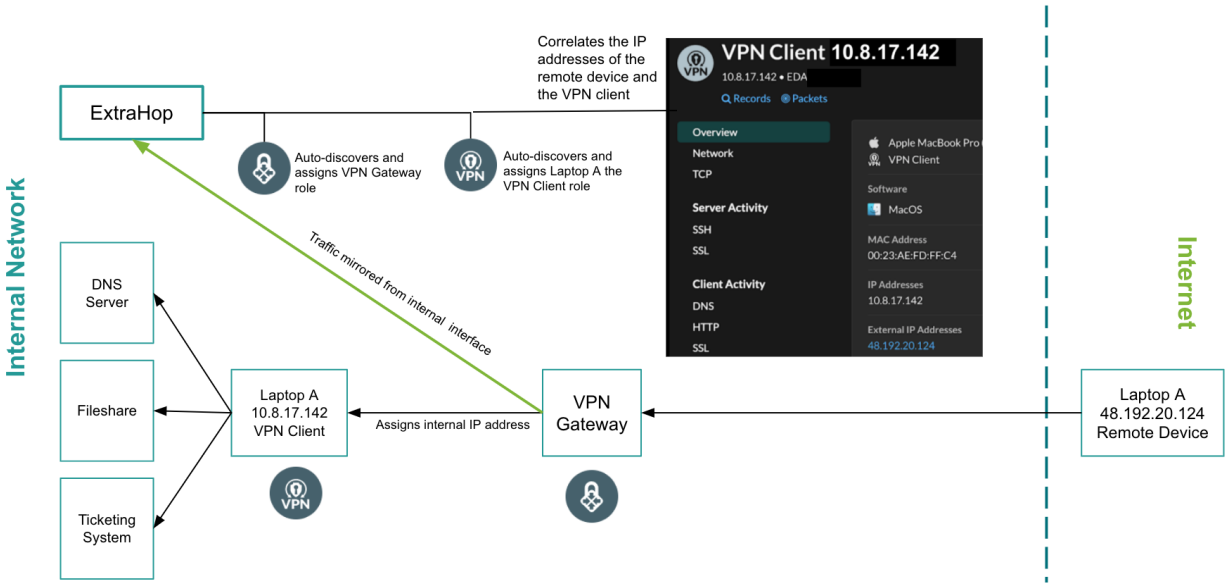
The ExtraHop Machine Learning Service aggregates WAN-side devices with active tunnels to a VPN gateway, analyzes traffic from both sides of the VPN gateway, and then automatically discovers and classifies these devices as VPN clients. You can then see the external and internal IP addresses for devices that are assigned the VPN Client role, and you can see the history for all IP addresses discovered by the system so that you can track when an IP address changes for a user.

The following system requirements must be met for VPN Discovery:

- The ExtraHop system must be connected to ExtraHop Cloud Services because VPN Discovery requires the Machine Learning Service.
- The ExtraHop system must be enabled for VPN Client Discovery.
- The ExtraHop system must have visibility to the internal and external interfaces on the VPN gateway.

VPN Discovery can only work when the ExtraHop system has access to both sides (or interfaces) of the VPN gateway. For most VPN gateways and in one-arm configurations, the ExtraHop system can automatically discover and assign the VPN Gateway role to devices on your network that are receiving VPN connections. Enable automatic classification and assignment of the VPN Gateway role in the running configuration file. If your VPN gateway is not classified by the system, you must manually assign the VPN Gateway role.

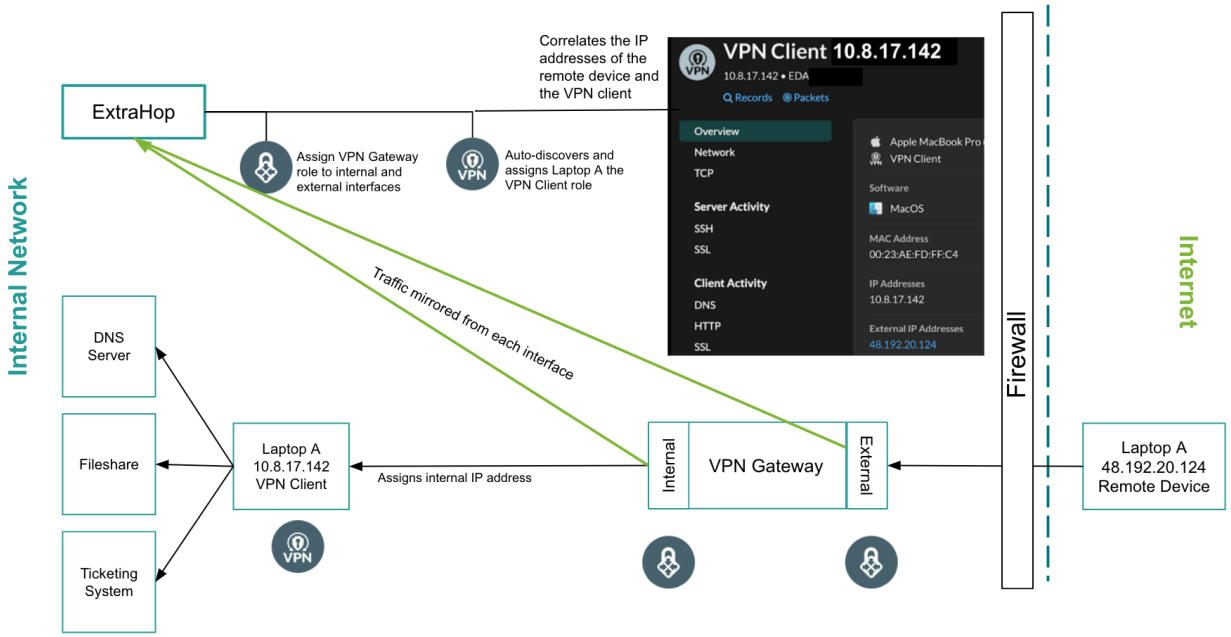
If the system assigns the VPN Gateway role to a router that is handling some VPN traffic, manually change the device role for the router to the Gateway role, and assign the VPN Gateway role to the correct device on your network.



The VPN Client device role is only assigned by the system to devices with an RFC-1918 (or private) IP address. These devices are automatically classified when they are discovered as a child of a VPN Gateway. The VPN Client role cannot be manually assigned.

Two-arm Configurations

For VPN gateways deployed in two-arm configurations, you must manually assign the VPN Gateway role to the internal interface of the VPN gateway; only the external interface is automatically classified by the ExtraHop system.



After the VPN gateway roles are assigned to the internal and external interfaces, the ExtraHop system automatically discovers VPN client devices for any RFC-1918 (or private) IP addresses that are assigned through the VPN gateway.

L2 and L3 Discovery

VPN Discovery works when the ExtraHop system is configured for either L2 Discovery or L3 Discovery.

- In L2 Discovery, VPN gateways are always classified as L2 devices and have a single device entry in the system.
- In L3 Discovery, both the L3 child entry and L2 parent entry for the VPN gateway are assigned the VPN Gateway role.

Segmented VPN gateways

If your VPN gateway is segmented in a way that does not allow traffic to be mirrored from both interfaces, you can collect observations through the ExtraHop REST API and manually associate internal-to-external traffic.