Comment fonctionne la mise en miroir

Publié: 2024-02-16

ExtraHop est un système passif.

Son flux de données filaire provient entièrement du trafic miroir. Il s'agit d'une amélioration par rapport aux méthodes traditionnelles de collecte de données filaires à l'aide d'analyseurs de paquets. Avec ExtraHop, le trafic est reflété directement dans le système, puis réassemblé pour former un trafic completclient sessions et flux de transactions, vous offrant l'intégralité de la charge utile des transactions en temps réel à analyser. Il existe deux manières de refléter le trafic dans ExtraHop : la mise en miroir basée sur le réseau et la mise en miroir basée sur l'hôte. Cette rubrique décrit les différences entre les deux.

Mise en miroir basée sur le réseau

Le principal avantage de la mise en miroir basée sur le réseau est que vous pouvez la configurer au niveau du réseau, en capturant le trafic provenant de plusieurs hôtes avec un minimum de configuration. Il existe différents types de mise en miroir basée sur le réseau, chacun étant conçu pour refléter le trafic vers une cible dans une situation particulière. Le principal défi de toutes les stratégies de mise en miroir basées sur le réseau est qu' elles reposent largement sur les capacités du matériel de votre réseau (physique ou virtuel). Si vous utilisez une appliance virtuelle ExtraHop, l'hyperviseur que vous utilisez (et même la version de l'hyperviseur) joue également un rôle dans l'équation. Cela dit, si vous pouvez tirer parti de la mise en miroir basée sur le réseau, vous devriez probablement le faire, car une fois configurée, sa maintenance nécessite moins d' efforts administratifs.

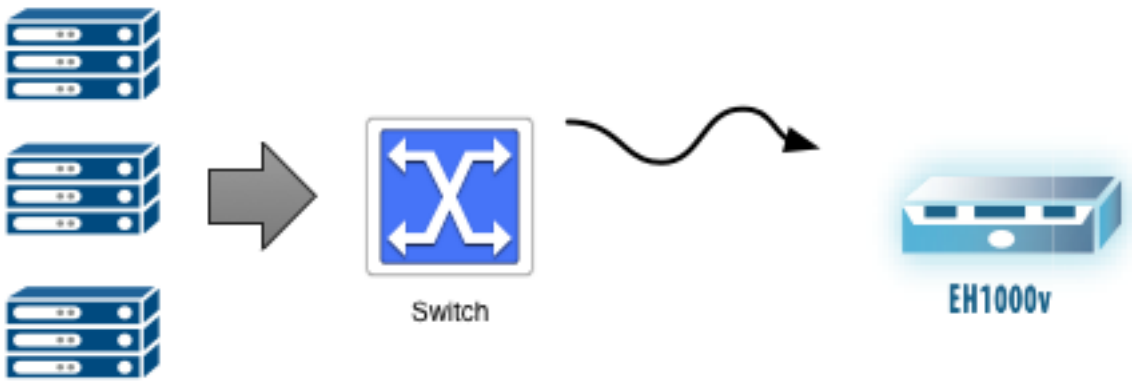
Il existe trois principaux types de mise en miroir basée sur le réseau.

Note: Si vous utilisez AWS, vous n'avez pas accès à la structure du réseau, ce qui signifie que la mise en miroir basée sur le réseau n'est pas disponible pour vous. Accédez plutôt à la section de mise en miroir basée sur l'hôte.

SPAN

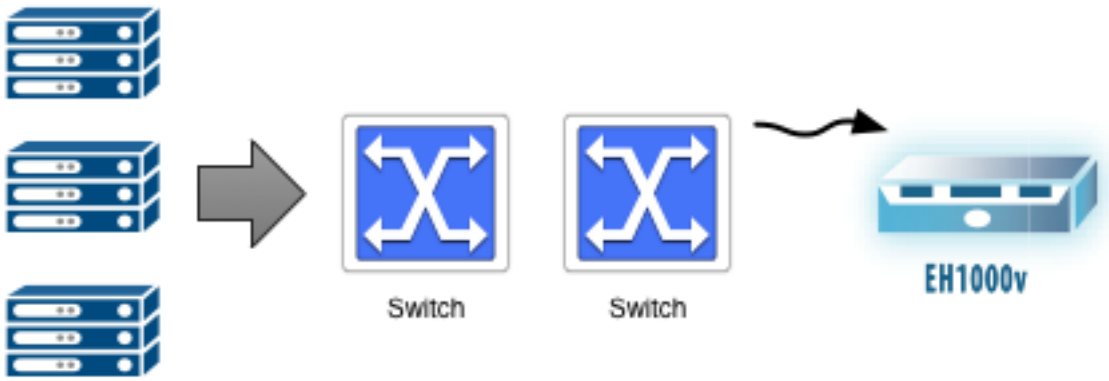
Le port SPAN est le nom du port sur les commutateurs Cisco qui reflète le trafic. SPAN est l'abréviation de Switched Port Analyzer (SPAN). Les différents fournisseurs portent des noms différents, mais le terme « spanning » est devenu synonyme de port sur un commutateur qui reflète le trafic. L'essentiel d'un SPAN est qu' il s'agit uniquement de trafic local. Vous pouvez configurer n'importe quel port du commutateur pour refléter le trafic vers un système ExtraHop ayant accès au port SPAN.

Le mode promiscueux est similaire au SPAN, mais au lieu de mettre en miroir uniquement le trafic local sélectionné sur le port SPAN, le mode promiscueux reflète tout le trafic provenant de chaque port. Tout le trafic qui passe par le commutateur est reflété sur votre système ExtraHop.



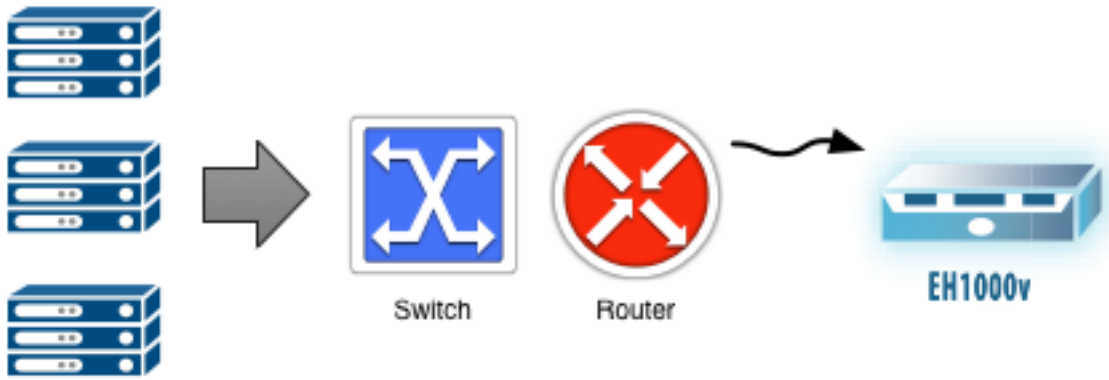
RSPAN

Le RSPAN est utile si le trafic que vous souhaitez mettre en miroir se trouve à plusieurs commutateurs de l'endroit où vous pouvez connecter votre système ExtraHop. Le « R » dans RSPAN signifie télécommande. Vous répartissez tout le trafic d'un commutateur à un certain nombre de commutateurs supplémentaires vers votre système ExtraHop cible à l'aide d'un VLAN de mise en miroir dédié. Chaque commutateur du chemin doit être configuré pour transporter le VLAN dédié qui contient le trafic miroir.



ERSPAN

Si une couche 3 (L3) une limite (telle qu'un routeur, un pare-feu ou un commutateur de couche 3) se situe entre le trafic que vous souhaitez refléter et l'endroit où vous pouvez connecter votre système ExtraHop, ERSPAN pourrait vous être utile. Pour franchir la limite de la couche 3, ERSPAN encapsule le trafic miroir dans un tunnel GRE adressé à l'adresse IP d'une interface de capture sur le système ExtraHop. Le trafic miroir encapsulé navigue sur le réseau comme le ferait n'importe quel autre paquet.



Miroir basé sur l'hôte

Si la mise en miroir basée sur le réseau ne fonctionne pas pour vous, la mise en miroir basée sur l'hôte est un moyen fiable d'acheminer du trafic vers le système ExtraHop.

Redirecteur de paquets

La mise en miroir basée sur l'hôte nécessite l'installation d'un redirecteur de paquets sur chaque hôte que vous souhaitez surveiller. Le gros avantage du redirecteur de paquets est qu'il fonctionne avec n'importe quel type d' équipement réseau dont vous disposez. Il fonctionne indépendamment du type ou de la version de l'hyperviseur que vous utilisez. La mise en miroir basée sur l'hôte est un moyen de configurer l'adaptateur sur un hôte pour dupliquer et transférer tout le trafic vers le système ExtraHop. Vous pouvez installer le logiciel de transfert de paquets sur des hôtes Windows et Linux.

Le transitaire de paquets (également appelé RPCAP et un robinet logiciel) est analogue à un robinet réseau, qui est un équipement matériel discret destiné à refléter le trafic provenant d'un réseau.