Fonctionnement de la mise en miroir

Publié: 2023-09-19

ExtraHop est un système passif.

Son alimentation en données filaires provient entièrement du trafic mis en 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 mis en miroir directement dans le système, puis réassemblé en sessions complètes par client et en flux de transactions, ce qui vous permet d'analyser en temps réel l'ensemble de la charge utile de la transaction. Il existe deux façons de mettre en miroir le trafic dans ExtraHop : la mise en miroir basée sur le réseau et la mise en miroir basée sur l'hôte. Cette rubrique traite des différences entre les deux.

Mise en miroir au niveau du réseau

Le grand avantage de la mise en miroir basée sur le réseau est qu'elle peut être mise en place au niveau du réseau, capturant le trafic de plusieurs hôtes avec un minimum de configuration. Il existe différents types de mise en miroir basée sur le réseau, chacun étant conçu pour mettre en miroir le trafic vers une cible dans une situation particulière. Le grand défi de toutes les stratégies de mise en miroir basée sur le réseau est qu'elles dépendent fortement des capacités du matériel de votre réseau (physique ou virtuel). Si vous utilisez une appliance ExtraHop virtuelle, 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 voudrez probablement le faire car, une fois mise en place, elle nécessite moins d'efforts administratifs pour être maintenue.

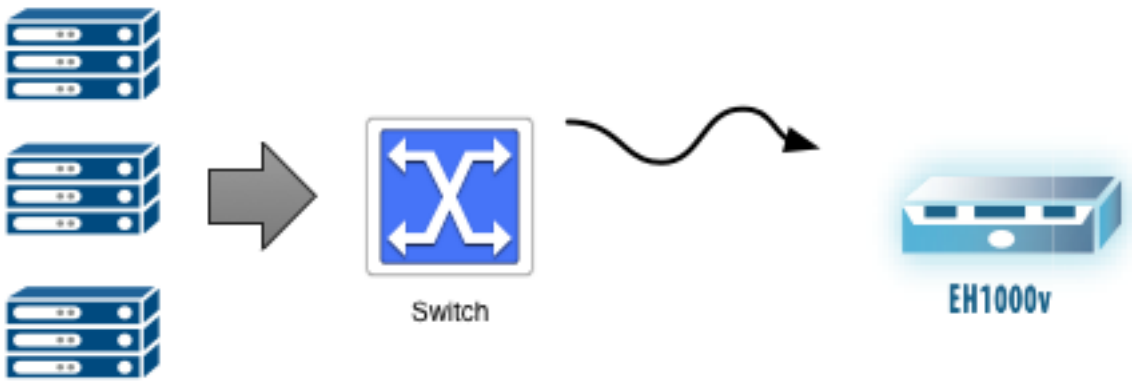
Il existe trois types principaux de mise en miroir basée sur le réseau

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. Passez plutôt à la section sur la mise en miroir basée sur l'hôte.

SPAN

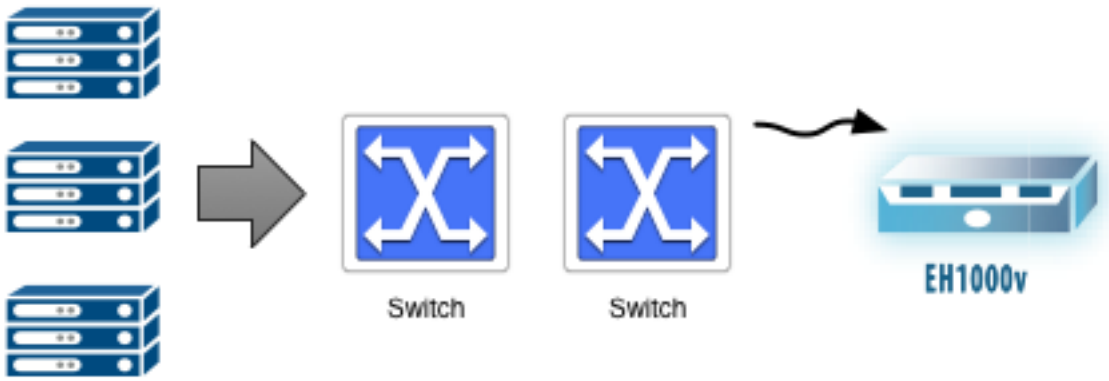
Le port SPAN est le nom du port des commutateurs Cisco qui reflète le trafic. SPAN est l'abréviation de Switched Port ANalyzer (SPAN). Les différents fournisseurs ont des noms différents, mais spanning est devenu synonyme d'un port sur un commutateur qui reflète le trafic. L'élément clé d'un SPAN est qu'il s'agit d'un trafic local. Vous pouvez configurer n'importe quel port du commutateur pour qu'il mette en miroir le trafic vers un système ExtraHop ayant accès au port SPAN.

Le mode promiscuous est similaire au SPAN, mais au lieu de mettre en miroir uniquement le trafic de certains ports locaux vers le port SPAN, le mode promiscuous met en miroir tout le trafic de chaque port. Tout le trafic qui passe par le commutateur est mis en miroir sur votre système ExtraHop.



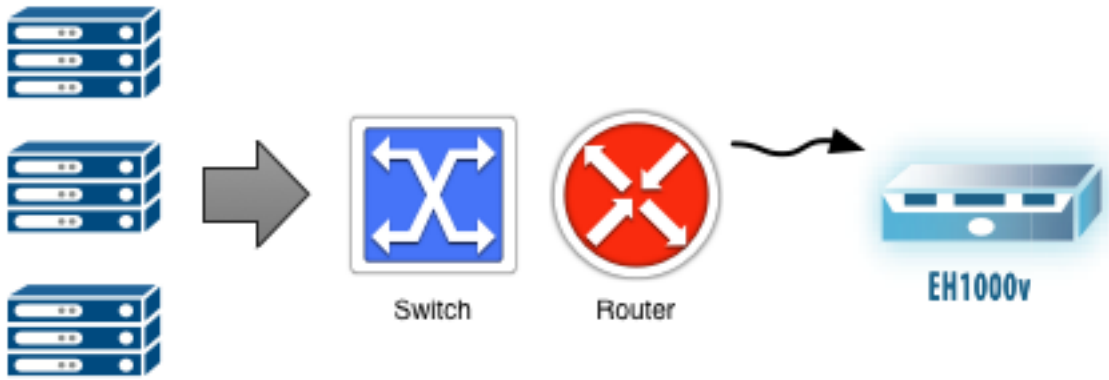
RSPAN

RSPAN est utile si le trafic que vous souhaitez mettre en miroir se trouve à plus d'un commutateur de l'endroit où vous pouvez attacher votre système ExtraHop. Le "R" de RSPAN signifie "distant". Vous étendez tout le trafic d'un commutateur à travers un nombre quelconque de commutateurs supplémentaires jusqu'à 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 frontière de couche 3 (L3) (telle qu'un routeur, un pare-feu ou un commutateur de couche 3) se trouve entre le trafic que vous souhaitez mettre en miroir et l'endroit où vous pouvez attacher votre système ExtraHop, ERSPANpeut vous être utile. Pour franchir la frontière 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 n'importe quel autre paquet.



Miroir basé sur l'hôte

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

Transmetteur 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 grand avantage du transmetteur de paquets est qu'il fonctionne avec n'importe quel type d'équipement réseau, indépendamment du type ou de la version de l'hyperviseur que vous utilisez. Il fonctionne indépendamment du type ou de la version de l'hyperviseur que vous utilisez. La mise en miroir basée sur l'hôte est une façon de configurer l'adaptateur sur un hôte pour dupliquer et

transmettre tout le trafic au système ExtraHop. Vous pouvez installer le logiciel de transfert de paquets sur les hôtes Windows et Linux.

Le transmetteur de paquets (également appelé RPCAP et prise logicielle) est analogue à une prise réseau, qui est un dispositif matériel discret permettant de mettre en miroir le trafic d'un réseau.