So funktioniert die Spiegelung

Veröffentlicht: 2024-07-02

ExtraHop ist ein passives System.

Sein wire data Datenfeed stammt ausschließlich aus gespiegeltem Verkehr. Dies ist eine Verbesserung gegenüber herkömmlichen Methoden zur Erfassung von wire data mit Paketanalysatoren. Mit ExtraHop wird der Traffic direkt in das System gespiegelt und dann wieder zu vollständigen Daten zusammengesetzt.Client Sessions und Transaktions-Streams, sodass Sie die gesamte Transaktions-Payload in Echtzeit analysieren können. Es gibt zwei Möglichkeiten, den Datenverkehr in ExtraHop zu spiegeln: netzwerkbasierte Spiegelung und hostbasierte Spiegelung. In diesem Thema werden die Unterschiede zwischen den beiden erörtert.

Netzwerkbasierte Spiegelung

Der große Vorteil der netzwerkbasierten Spiegelung besteht darin, dass Sie sie auf Netzwerkebene einrichten können, sodass der Datenverkehr von mehreren Hosts mit einem minimalen Konfigurationsaufwand erfasst wird. Es gibt verschiedene Arten der netzwerkbasierten Spiegelung, die jeweils für die Spiegelung des Datenverkehrs zu einem Ziel in einer bestimmten Situation konzipiert sind. Die große Herausforderung bei allen netzwerkbasierten Spiegelungsstrategien besteht darin, dass sie stark von den Fähigkeiten der Hardware in Ihrem Netzwerk (physisch oder virtuell) abhängen. Wenn Sie eine virtuelle ExtraHop-Appliance ausführen, spielt auch der von Ihnen verwendete Hypervisor (und sogar die Version des Hypervisor) eine Rolle. Wenn Sie jedoch die Vorteile der netzwerkbasierten Spiegelung nutzen können, werden Sie dies wahrscheinlich tun wollen, da nach der Einrichtung weniger Verwaltungsaufwand für die Wartung erforderlich ist.

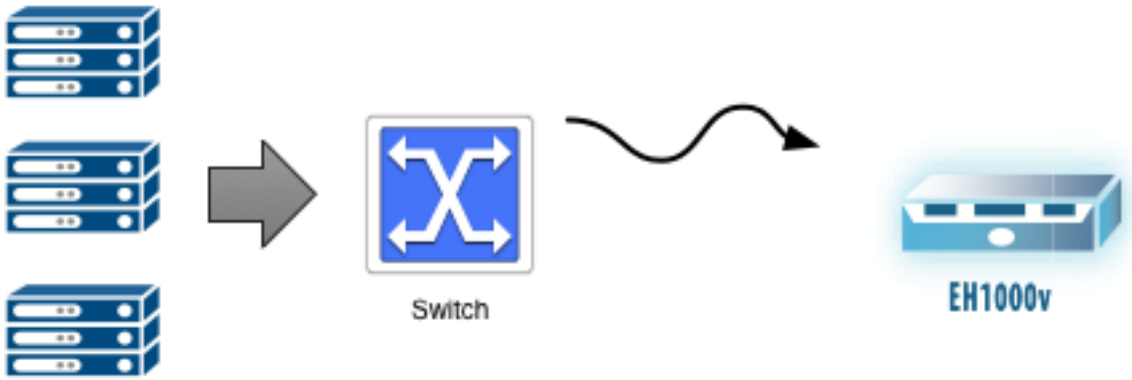
Es gibt drei Haupttypen der netzwerkbasierten Spiegelung.

Hinweis: Wenn Sie AWS verwenden, haben Sie keinen Zugriff auf die Netzwerkstruktur, was bedeutet, dass die netzwerkbasierte Spiegelung für Sie nicht verfügbar ist. Gehen Sie stattdessen zum Abschnitt hostbasierte Spiegelung.

SPAN

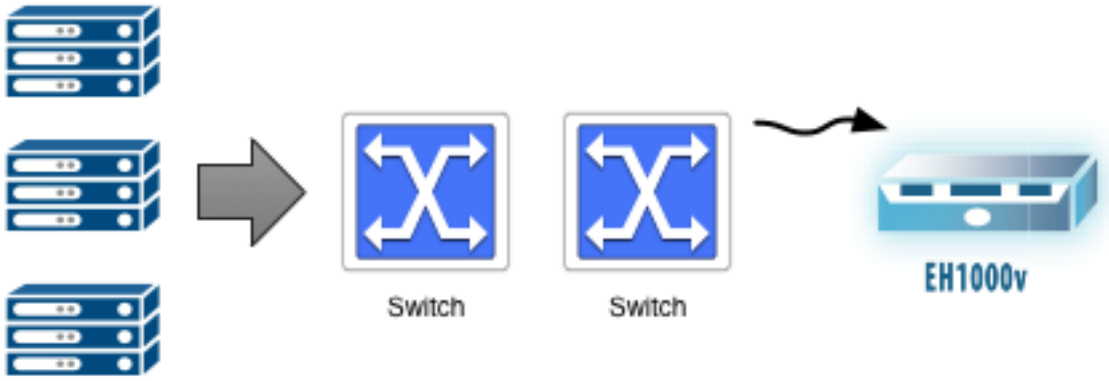
Der SPAN-Port ist der Name des Ports auf Cisco Switches, der den Datenverkehr widerspiegelt. SPAN steht für Switched Port Analyzer (SPAN). Verschiedene Anbieter haben unterschiedliche Namen, aber Spanning ist zum Synonym für einen Port auf einem Switch geworden, der den Datenverkehr widerspiegelt. Das Wichtigste an einem SPAN ist, dass es sich ausschließlich um lokalen Verkehr handelt. Sie können jeden der Ports am Switch so konfigurieren, dass er den Datenverkehr auf ein ExtraHop-System spiegelt, das Zugriff auf den SPAN-Port hat.

Der Promiscuous-Modus ähnelt SPAN, aber anstatt nur ausgewählten lokalen Port-Verkehr zum SPAN-Port zu spiegeln, spiegelt der Promiscuous-Modus den gesamten Verkehr von jedem Port wider. Jeglicher Traffic, der über den Switch kommt, wird auf Ihr ExtraHop-System gespiegelt.



RSPAN

RSPAN ist nützlich, wenn der Datenverkehr, den Sie spiegeln möchten, mehr als einen Switch von der Stelle entfernt ist, an der Sie Ihr ExtraHop-System anschließen können. Das „R“ in RSPAN steht für Remote. Sie übertragen den gesamten Datenverkehr von einem Switch über eine beliebige Anzahl zusätzlicher Switches zu Ihrem ExtraHop-Zielsystem mithilfe eines dedizierten Spiegelungs-VLANs. Jeder Switch im Pfad muss so konfiguriert werden, dass er das dedizierte VLAN überträgt, das den Spiegeldatenverkehr enthält.



ERSPAN

Wenn eine Schicht 3 (L3) Die Grenze (z. B. ein Router, eine Firewall oder ein Layer-3-Switch) liegt zwischen dem Datenverkehr, den Sie spiegeln möchten, und dem Ort, an den Sie Ihr ExtraHop-System anschließen können, ERSPAN könnte für dich hilfreich sein. Um die Layer-3-Grenze zu überschreiten, kapselt ERSPAN den Spiegelverkehr in einem GRE-Tunnel, der an die IP-Adresse einer Capture-Schnittstelle auf dem ExtraHop-System adressiert ist. Der gekapselte Spiegelverkehr navigiert im Netzwerk genauso wie jedes andere Paket.

Host-basierte Spiegelung

Wenn die netzwerkbasierte Spiegelung für Sie nicht funktioniert, ist die hostbasierte Spiegelung eine zuverlässige Methode, um Datenverkehr in das ExtraHop-System zu leiten.

Paketweiterleitung

Für die hostbasierte Spiegelung müssen Sie auf jedem Host, den Sie überwachen möchten , eine Paketweiterleitung installieren. Der große Vorteil des Paket Forwarders besteht darin, dass er mit jeder Art von Netzwerkausrüstung funktioniert, die Sie haben. Es funktioniert unabhängig vom Typ oder der Version des Hypervisor, den Sie ausführen. Host-basierte Spiegelung ist eine Möglichkeit, den Adapter auf einem Host so zu konfigurieren, dass er den gesamten Datenverkehr dupliziert und an das ExtraHop-System weiterleitet. Sie können die Paket Forwarder-Software auf Windows- und Linux-Hosts installieren.

Der Paket Forwarder (auch genannt RPCAP und ein Software-Tap) entspricht einem Netzwerk-Tap, bei dem es sich um ein unauffälliges Hardwaregerät zur Spiegelung von Datenverkehr aus einem Netzwerk handelt.