

GENAUE KOPIE VON SCHNITTSTELLEN

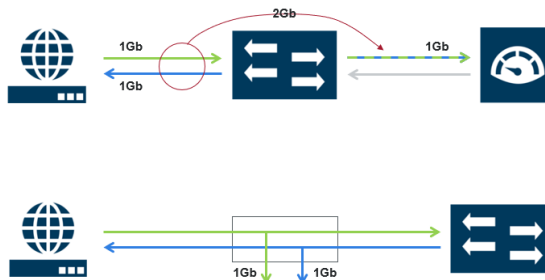
PROBLEM:

Beim Anfertigen von Kopien des Datenverkehrs wird oft auf die Mirror-Port-Technologie oder deren Umsetzung von Cisco, SPAN (Switched Port Analyzer) oder RSPAN (Remote Span) zurückgegriffen. Diese Technologie war aber nie dazu gedacht, dauerhaft Kopien vom Datenverkehr anzufertigen, sondern für Troubleshooting-Aufgaben. Die Anfertigung von Datenverkehrskopien mit Mirror/Span ist schlicht unmöglich, da die Kommunikationen in den Kommunikationsleitungen bidirektional sind, und ein Port Mirror nie eine 1 Gb große bidirektionale Leitung auf eine 1 Gb große unidirektionale Leitung kopieren können wird.

Wir könnten dazu verleitet werden anzunehmen, dass die Leitung nicht komplett voll ist und die Überschreibung kein Problem darstellen würde, aber wenn die Spitzenwerte des eingehenden und ausgehenden Verkehrs die Kapazität der Schnittstelle übersteigen, werfen wir Datenverkehr über Bord, was im Fall von zustandhaften Empfangsgeräten den Verlust der gesamten Sitzung bedeutet. Wenn es sich um eine Sicherheitsanwendung handelt, kann der Verlust eines einzigen Pakets katastrophal sein.

Zuletzt werden wir, wenn wir die Kapazitäten unseres Switching/Routing-Herstellers recherchieren, feststellen, dass alle Hersteller Schutzmaßnahmen an den Geräten einsetzen, sodass, wenn ein bestimmter Schwellenwert an Datenverkehr in der gespiegelten Leitung überschritten wird, auf die Schnittstelle zurückgegriffen wird, um die Hauptaufgabe des Geräts nicht zu gefährden.

SCHEMA:



GENAUE KOPIE VON SCHNITTSTELLEN

LÖSUNG:

Die einzige Lösung, die wirklich den Datenverkehr, und zwar den gesamten Datenverkehr eines Links kopiert, sind TAPs (Test Access Port). Dabei handelt es sich um Geräte, die im „T“-Modus agieren: Sie werden in eine Kommunikationsleitung eingesetzt und erstellen eine exakte Kopie des Datenverkehrs.

So wird eine bidirektionale Kommunikationsleitung von dem TAP in 2 unidirektionale Leitungen der gleichen Kapazität umgewandelt, sodass eine vollständige Kopie des Datenverkehrs erstellt werden kann.

Es gibt verschiedene Arten von TAPs, je nach dem physischen Medium, über das die Kopie des Datenverkehrs erstellt werden soll:

- Passive (über Faserschnittstellen): Dabei handelt es sich um Geräte ohne Betriebssystem, Versorgung oder SW, die lediglich das Licht zwischen der Hauptleitung und der Kopie aufteilen. Im Grunde stellen sie also einfache optische Prismen dar.
- Aktive (für Kupferschnittstellen): Gleichwertig mit den zuvor genannten, aber sie erfordern eine Versorgung für die Kupferschnittstelle.
- Virtuelle: Um Datenverkehr aus virtuellen Umgebungen zu erfassen, verfügt Gigamon über SW, die Datenverkehr aus AWS, Azure, GCP, VMWare (ESX/NSX/NSX-T), Openstack, Nutanix und Kubernetes-Umgebungen entnehmen können.

LIZENZEN:

- TAPs
- vTAPs