Copie effettive di Interfacce

Problema

Per realizzare copie del traffico in molti casi si ricorre alla tecnologia di port mirror, o, alla sua implementazione Cisco, SPAN (Switched port analyzer) o RSPAN (remote span). Questa tecnologia non è stata però progettata per realizzare copie di traffico in modo permanente, ma per funzioni di troubleshooting.
Realizzare copie del traffico con mirror/span è semplicemente impossibile, perché le comunicazioni sulle linee sono bidirezionali, e un port mirror non potrà mai copiare una linea bidirezionale da 1 Gb su una linea monodirezionale da 1 Gb.
Potremmo cadere nella tentazione di pensare che la linea non sia completamente piena e che non ci saranno problemi di eccesso di scrittura, ma quando i picchi di traffico in ingresso e uscita supereranno la capacità dell'interfaccia, parte del traffico sarà tralasciata, e questo comporterà la perdita di tutta la sessione qualora il dispositivo di ricezione sia statefull. Nel caso in cui si tratti di un'applicazione di sicurezza, perdere anche solo un pacchetto può avere conseguenze catastrofiche.
Infine, se ci interroghiamo sulle capacità del nostro produttore di switching/routing scopriremo che tutti i fabbricanti implementano misure di protezione dei loro dispositivi perché se si supera un certo volume di traffico sulla linea del mirror, tralascino l'interfaccia, in modo da non mettere a rischio la funzione principale del dispositivo.

Soluzione

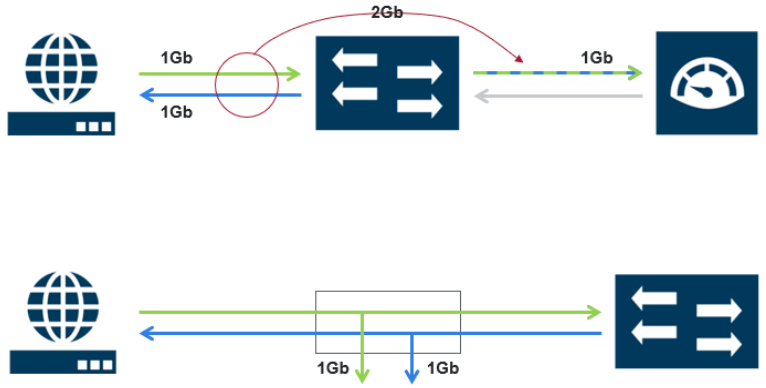
L'unica soluzione che davvero copia il traffico, e tutto il traffico di un link, sono i TAP (Test Acces Port). Si tratta di dispositivi che agiscono come "T": si collegano a una linea di comunicazione ed estraggono una copia esatta del traffico.

In questo modo, una linea bidirezionale di comunicazione viene convertita dal TAP in 2 linee monodirezionali di pari capacità, per cui viene estratta la copia esatta del traffico.

Esistono vari tipi di TAP, in base allo strumento fisico su cui si desidera estrarre la copia del traffico:

- Passivi (per interfacce in fibra): si tratta di un dispositivo privo di sistema operativo, alimentazione e SW, che semplicemente divide la corrente tra la linea principale e quella per la copia. In effetti, è un semplice prisma ottico
- Attivi (per interfacce in rame): equivalenti ai precedenti, ma richiedono alimentazione per la propria interfaccia in rame
- Virtuali: per catturare traffico in ambienti virtuali, Gigamon dispone di un SW capace di estrarre traffico in ambienti AWS, AWS, Azure, GCP, VMWare (ESX/NSX/NSX-T), Openstack, Nutanix, Kubernetes

Schema



Licenze

TAP
vTAP

LINK