SPAN de ports vs TAP pour copie du trafic

Les sondes de performance et de détection des menaces de sécurité par analyse des flux en ligne nécessitent leur raccordement via des technologies de copie garantissant une image fidèle du trafic analysé.
Copie de ports ou déploiement de TAP sur les réseaux à surveiller, il s'agit de faire le bon choix.
Ce livre blanc vise à faire un point objectif sur les deux technologies.

Deux méthodes très différentes

- SPAN

Le span de ports est une fonction embarquée dans les équipements actifs tels que switches et routeurs. Elle s'active par lignes de commandes CLI ou logiciels embarqués. Le principe consiste à paramétrer l'équipement de manière à rediriger la copie du trafic échangé vers des ports disponibles sur lesquels les outils d'analyse sont connectés.
Sa simplicité de mise en œuvre et sa rapidité à dupliquer le trafic en s'appuyant sur les équipements du réseau déjà déployés en production en font une solution privilégiée des ingénieurs et techniciens IT.
Suivant le modèle OSI, la copie se fait aux niveaux 2 et 3.

- TAP

L'utilisation de TAP (Test Access Point) est l'alternative au SPAN. Un TAP est un boîtier physique totalement passif. Il permet d'obtenir une copie des flux Rx et Tx du lien sur lequel il est inséré vers deux ports dédiés de sortie, l'un pour le trafic Rx et l'autre pour le trafic Tx. Cette copie est une copie fidèle de la couche physique analysée vers une couche physique identique. Par exemple, un TAP positionné sur un lien optique multimode transmettra une copie du trafic vers deux ports accessibles eux-mêmes en fibre multimode (un port pour le Rx et un port pour le Tx).
Un TAP est positionné en coupure du lien en surveillance et nécessite donc une interruption planifiée temporaire du trafic lors de son insertion.
Le TAP est moins privilégié dans les environnements IT de par cette nécessité de couper physiquement le lien afin d'y insérer l'équipement.

Avantages et contraintes des deux méthodes de copie

- SPAN

Pour la plupart des besoins de supervision simples et lorsqu'aucune architecture de copie n'a été prévue sur le réseau en production, les fonctionnalités de Span permettent de répondre rapidement aux besoins de copie. Aucune intervention physique n'est à prévoir et toutes les opérations d'activation peuvent se réaliser à distance en s'appuyant sur les logiciels des équipements .
Toutefois, ces fonctions sont consommatrices de CPU et il est donc important de vérifier que les ressources nécessaires à leur activation sont disponibles. De plus, sur des équipements de production, le risque inhérent à des erreurs de paramétrage lors de modifications de configurations n'est jamais négligeable. Les exemples de défauts de production liés à de telles opérations sont significatifs et il est important de s'assurer que les procédures internes relatives à la gestion des configurations sont respectées. Enfin, dans le cas d'analyses de performance sur les flux échangés, l'impact du SPAN sur la CPU peut parfois être considéré comme lui-même source de ralentissements.

En termes d'inconvénients majeurs, se pose la question des ports de sorties en surcharge entraînant une perte des données recopiés, mais surtout, il est important de garder à l'esprit que, de par son principe même de copie aux niveaux 2 et 3, certaines informations peuvent ne pas être transmises.

Elles concernent principalement :

- les erreurs de bas niveau, type CRC (nécessaires à la détection d'attaques *Click* ou *Win Newk, winfreez*)
- les tailles de paquets trop petites
- les tailles de paquets trop grosses (nécessaires pour détection des *Deny of service* tel que *fragment attack, ping of death*)
- Les paquets corrompus (nécessaires à la détection d'attaques *BONK, BOINK, Teardrop*).

- TAP

Le TAP réalisant une copie physique du trafic, il est la garantie de ce qu'aucune information du paquet copié ne soit masquée ou filtrée. Il est totalement passif vis-à-vis du lien en production sur lequel il est inséré. Les trafics Rx et Tx sont physiquement dissociés. L'utilisation du TAP ne présente aucun impact sur les équipements actifs.

Pour des analyses à des fins sécuritaires, il est la seule technologie qui garantisse une vision intégrale de tous les paquets

L'unique défaut du TAP, et celui-ci a son importance, réside dans son déploiement. Positionné en insertion sur les liens en surveillance, il nécessite d'être planifié et une intervention physique sur le lien doit être organisée. Il est ainsi parfois compliqué d'envisager son installation lors de campagnes d'analyses ponctuelles.

SYNTHÈSE DU COMPARATIF TAP VS SPAN

	TAP	SPAN	Commentaires
Mise en œuvre	Nécessite coupure des liens à analyser	Nécessite droits en modification de paramétrage sur les équipements switchs ou routeurs	TAP : planification de coupure physique des liens SPAN : modifications logicielles sur les équipements
Agilité	Peu agile	Très agile	
Incidence / Passivité	Totalement passif après insertion	Consommation de ports et de CPU sur les équipements	SPAN : risques sur la production liés aux éventuelles surcharges de CPU mais surtout aux opérations de modifications des configurations sur les équipements actifs
Fiabilité des informations recopiées	Copie intégrale de toutes les informations échangées sur le lien physique analysé	Perte d'informations liées aux paquets eux-mêmes (paquets malformés, corrompus, en erreur, etc…) empêchant la détection de certaines attaques	A étudier attentivement suivant le type d'analyse à réaliser
Types d'analyses (performance / sécurité)	Parfaitement adapté pour tous les types d'analyses sans aucune perte d'informations	Globalement adapté pour les analyses de performance mais peu adapté pour les analyses de sécurité	Pour les analyses de sécurité, voir les recommandations de l'ANSSI sur les préconisations à l'installation de TAP

allentis
info@allentis.eu
www.allentis.eu
140bis, rue de Rennes
75006 Paris -France
Tél. : +33 1 70 38 25