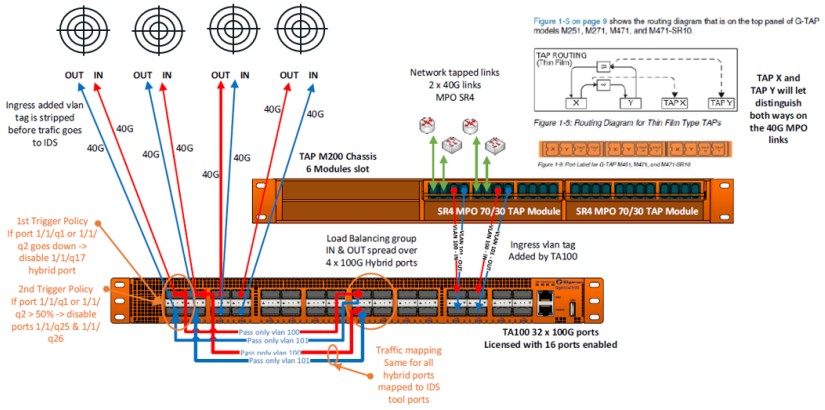
ZENTRALISIERUNG UND ENTLASTUNG DES IDS

PROBLEM:

Die Tools des Intrusion Detection Systems (IDS) sind bei der Erkennung von Angriffen auf Basis der Analyse von Signaturen und Trafficverhalten äußerst wirkungsvoll, aber ihre Bereitstellung stellt eine erhebliche Herausforderung dar, wenn unsere Infrastruktur geografisch verstreut ist. Die Bereitstellung von Sonden an jedem einzelnen Standort der Organisation ist nicht zweckmäßig, weder im Hinblick auf die Kosten, die investiert werden müssten, noch in Bezug auf den Verwaltungsaufwand.
Zudem werden diese Tools nach der Bandbreite dimensioniert, die sie empfangen, und ihre Leistung wird erheblich beeinträchtigt, wenn verschlüsselter Datenverkehr empfangen wird.

SCHEMA:



Exclusive Networks Austria GmbH I Heinrich Bablik-Straße 17 K21 Top N06 I 2345 Brunn am Gebirge
Tel +43 (1) 336 0 337 - 0 I info.at@exclusive-networks.com

ZENTRALISIERUNG UND ENTLASTUNG DES IDS

LÖSUNG:

Um die Kosten der Bereitstellung der IDS-Sonden zu rationalisieren, bieten die NPB-Lösungen von Gigamon diverse Alternativen

Zur Reduzierung der Bandbreite, die an das IDS gesendet wird

- Reduktion des Datenverkehrs, der an die Sonde gesendet wird, basierend auf L2-3-4-7-Filtern
- Einsatz von Advance Slicing für den Versand der ersten Pakete jeder Sitzung und Verwerfen des Rests der Sitzung, wenn dieser nicht sicherheitsrelevant ist.
- SSL-Entschlüsselung vor dem Versand an die Sonde

Zur Zentralisierung des Datenverkehrs in zentralen Sonden

- Erstellung von Kopien des relevanten Traffic über TAPs an entfernten Standorten für den Transport zur Zentrale und Konsolidierung in den zentralisierten Sonden
- Filterung des Datenverkehrs am Ursprungsort, wenn die Transportbandbreite begrenzt ist und Tunneling des Datenverkehrs bis zum zentralen Punkt

LIZENZEN:

- Flow Mapping
- Load Balancing
- Tunneling
- Application Filter Intelligence
- Advance Slicing
- SSL Decryption

Exclusive Networks Austria GmbH I Heinrich Bablik-Straße 17 K21 Top N06 I 2345 Brunn am Gebirge
Tel +43 (1) 336 0 337 - 0 I info.at@exclusive-networks.com