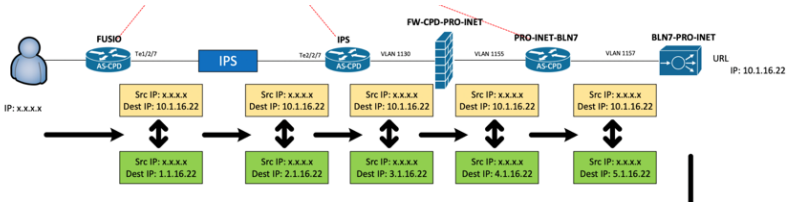
MODIFIZIERUNG VON PAKETEN FÜR „FALSCHE“ NPM/NAT

PROBLEM:

NPM-Tools sind für das Monitoring der Qualität der Benutzererfahrung in einem Netzwerk äußerst nützlich. Aber um die Daten aus der Datenverkehrserfassung korrekt zu analysieren, sei es anhand von Span/Mirror/Tap oder Metdadaten-Protokollen wie Netflow, muss diese Information von dem Tool interpretierbar sein, was oft nicht möglich ist.

Ein typisches Szenario ist, dass wir die Servicequalität in einem der auf Niveau 2 bereitgestellten Geräte anhand eines NPM-Tools monitoren möchten, welche erfordert, dass eine Änderung auf Niveau 3 zugrunde liegt, um den Gerätesprung zu erkennen. Da sich die Geräte auf Niveau 2 befinden, sieht das NPM nur ein Paket, das die gesamte Gerätekette durchläuft, ohne die Sprünge zu erkennen, die zwischen den verschiedenen Geräten stattgefunden haben, und erkennt daher nicht die Qualitätsprobleme des Netzwerks.

SCHEMA:



Exclusive Networks Deutschland GmbH I Hardenbergstraße 9a I 10623 Berlin
Tel +49 (30) 325131 - 0 I info@exclusive-networks.de

MODIFIZIERUNG VON PAKETEN FÜR „FALSCHE“ NPM/NAT

LÖSUNG:

Obwohl die Masking-Funktion der GigaSMART-Karte von Gigamon ursprünglich entwickelt wurde, um vertrauliche Informationen in den Paketen zu verwischen, ermöglicht sie es uns auch, jeden anderen Parameter des Pakets zu ändern, indem ein bestimmtes Offset neben den gewünschten Änderungen festgelegt wird.

So können die IP-Adresse oder ein Teil dieser geändert werden, um eine „falsche“ NAT zu generieren, die es den NPM-Geräten ermöglicht, die zwischen den Geräten stattgefundenen Sprünge richtig zu erkennen und jene Geräte korrekt zu identifizieren, die für Verzögerungen, Verluste usw. verantwortlich sind.

LIZENZEN:

- Masking

Exclusive Networks Deutschland GmbH I Hardenbergstraße 9a I 10623 Berlin
Tel +49 (30) 325131 - 0 I info@exclusive-networks.de