Analyse réseau

L'analyse réseau dans NetExpert est basée sur un moteur d'analytiques réseau qui utilise les flows pour agréger les données. Bien que les valeurs ne soient pas 100% précises, les ratios sont fiables et permettent une analyse efficace du trafic réseau.

Définition de l'analyse réseau

L'analyse réseau permet de mesurer et d'analyser le trafic qui passe par votre réseau. Cela inclut toutes les informations principales des paquets, IPs, Ports, Protocoles, ASN, Pays

Fonctionnalités de l'analyse réseau

NetExpert offre plusieurs fonctionnalités pour l'analyse réseau :

- **Visualisation des flux** : Permet de visualiser les flux de trafic pour identifier les zones de congestion et les anomalies.
- **Analyse du trafic** : Permet d'analyser le trafic en fonction de la source, de la destination et de l'ASN.
- **Rapports exportables pour audits** : Permet d'exporter des rapports pour des audits ou des analyses ultérieures.

Moteur de filtres

Langage de filtrage

Le langage de filtrage de NetExpert est similaire à SQL avec quelques variations. Les champs listés comme dimensions peuvent généralement être utilisés. Les opérateurs acceptés sont =, !=, <, <=, >, >=, IN, NOTIN, LIKE, UNLIKE, ILIKE, IUNLIKE, <<, et !<<, lorsque cela est applicable. Voici quelques exemples :

- `srcPort = 443` sélectionne les flux où le port source est **443**. La valeur ne doit pas être entre guillemets.
- `SrcAS = AS12322`, `SrcAS = 12322`, ou `SrcAS IN (12322, 29447)` limite le numéro AS source des flux sélectionnés.
- `SrcAddr = 203.0.113.4` sélectionne uniquement les flux avec l'adresse spécifiée. Notez que le filtrage sur les adresses IP est généralement plus lent.
- `SrcAddr << 203.0.113.0/24` sélectionne uniquement les flux qui correspondent au sous-réseau spécifié.

Les noms de champs ne sont pas sensibles à la casse.

Notez que l'utilisation des champs suivants empêchera l'utilisation de données agrégées et sera donc plus lente :

- `SrcAddr` et `DstAddr`
- `SrcPort` et `DstPort`

Dimensions

Vous pouvez sélectionner un ensemble de dimensions. Pour les séries temporelles, les dimensions sont converties en séries. Elles sont empilées avec "stacked", affichées sous forme de lignes simples avec "lines". Pour les graphiques de Sankey, les dimensions sont converties en nœuds. Dans ce cas, vous devez sélectionner au moins deux dimensions.

L'ordre de sélection est important pour les dimensions.

Revision #1
Created 2025-12-06 14:10:08 UTC by Landry JUGE
Updated 2025-12-06 14:19:19 UTC by Landry JUGE