NETWORK TRAFFIC ANALYZER

blësk network monitoring

OBJECTIF : Colliger les données de manière continue, afin de centraliser l'information qui révèle à quel escient les ressources du réseau sont utilisées.

Votre réseau est lent, vos usagers se plaignent, votre équipe TI est débordée et en mode panique, car elle n'arrive pas à trouver la source du problème ? Savez-vous si vos utilisateurs contournent vos règles de pare-feu pour accéder à des sites non autorisés par la compagnie ?

BLËSK Network Traffic Analyzer (NTA) vous permet d'analyser, en temps réel, l'information concernant les données transigées sur le réseau. L'information obtenue peut être disséquée au besoin selon la recherche entreprise :

- Quels sont les protocoles les plus utilisés ?
- Quels équipements interagissent entre eux ?
- Qui utilise le plus de bande passante ?

BÉNÉFICES

- Trier le trafic réseau en fonction de nombreux critères.
- Afficher le trafic réseau en temps réel et les hôtes actifs.
- Produire des rapports à long terme pour plusieurs métriques du réseau.
- Surveiller et signaler le débit en direct, les latences du réseau et d'application, etc.
- Stocker sur disque des statistiques de trafic persistantes pour permettre des explorations futures et des analyses post-mortem.
- Géolocaliser et superposer des hôtes sur une carte géographique.

BLËSK VOUS AIDE:

NTA agit comme un « *sniffer* » en temps réel grâce au projet Open Source appelé Ntopng. Ntopng est une sonde de trafic réseau qui surveiller l'utilisation du réseau. Celui-ci fournit une interface utilisateur Web intuitive et cryptée pour l'exploration des informations en temps réel et l'historique du trafic des données.

De plus, Ntopng utilisé par NTA de BLËSK permet de découvrir les protocoles d'application (Facebook, Youtube, BitTorrent, etc.) en s'appuyant sur l'approche nDPI, une technologie d'inspection de paquet en profondeur. Il caractérise le trafic HTTP en s'appuyant sur les services de caractérisation fournis par Google et la liste noire HTTP. Ntopng analyse le trafic IP et le trie en fonction de sa source/destination. Vous pouvez aussi faire une exploration interactive des données surveillées et exportées vers MySQL puis recevoir des alertes pour capturer les hôtes anormaux et suspects.