GESTION DE FLUX AVEC NETFLOW ET NFSEN

i RENALA

Research and Education Network for Academic and Learning Activities

Le NREN Malgache

PLAN

- Introduction sur netflow
  - Flux de réseau
  - Travailler avec les Flux
  - Descripteurs de flux
  - Version Netflow
  - Utilisations des flux
- Présentation de Nfsen
  - Alertes et stats de Nfsen
  - Utilisation de Nfsen
- Conclusion

Flux de réseau

- Paquets ou trames présentant un attribut commun.
- Politique de création et d'expiration

– conditions de démarrage et d'arrêt d'un flux.

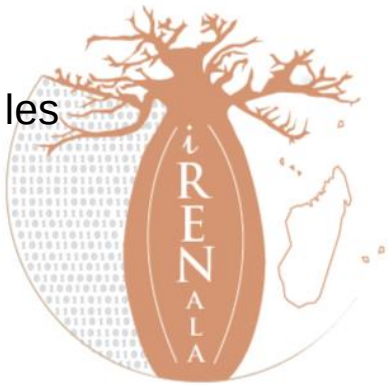
- Compteurs

– paquets, octets, temps.

- Informations d'acheminement

– système autonome (AS), masque de réseau, interfaces.

- Unidirectionnels ou bidirectionnels.
- Les flux bidirectionnels peuvent contenir d'autres informations telles que le temps d'aller-retour, le comportement TCP.
- Les flux d'application regardent au-delà des en-têtes afin de classifier les paquets en fonction de leur contenu.
- Flux agrégés – flux de flux.



Travailler avec les Flux

- Génération et affichage des flux
- Exportation de flux à partir de périphériques
  - Types de flux
  - Taux d'échantillonnage
- Collecte
  - Outils de collecte de flux
  - Outils de flux
- Analyse
  - Utiliser les outils existants ou en créer

Descripteurs de flux

- Plus la clé comporte d'éléments plus elle génère de flux.
- Un nombre supérieur de flux signifie :
  - Plus de temps de post-traitement pour générer les rapports
  - Plus de mémoire et de capacité d'UC pour les équipements générateurs de flux.
- Dépendant de l'application. Ingénierie du trafic ou détection des intrusions.

VERSION NETFLOW

- Version netflow dans pfsense (1, 5, 9).
- Chaque version se caractérise par son propre format de paquets.
- La version 1 ne comporte pas de numéros de séquence – aucun moyen de détecter les flux perdus.
- La “version” détermine le type de données du flux.

UTILISATIONS DES FLUX

- Identification / résolution des problèmes

  Classification du trafic

  Traçage des dénis de service (quelques diapositives de Danny McPherson)

- Analyse du trafic

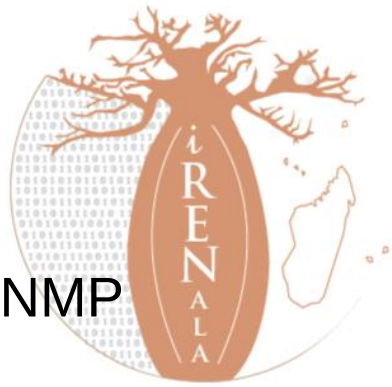
  Analyse du trafic inter-AS (systèmes autonomes)

  Rapport sur les serveurs mandataires (proxies)

- Comptabilisation

  Vérification croisée à partir d'autres sources

  – Possibilité de vérification croisée avec les données SNMP



PRÉSENTATION DE NFSEN

- Un outil graphique qui sert d'interface à **NfDump**
  - Le **NfDump** est un outils qui permet de collecter et traiter les données **netflow** au niveau de la Commande Line Interface (CLI)
- **Nfsen** permet de:

  - Naviguer facilement dans les flux NetFlow

  - Analyser les données netflow dans un intervalle de temps donné

  - Créer un historique ainsi que des profils d'analyse

  - Régler des alertes, en fonction des conditions

  - Écrire vos propres extensions pour traiter les données à intervalles réguliers.

ALERTES ET STATS DE NFSEN

- Page d'alerte
  - Créer des alertes en fonction de seuils définis, ex: montée ou baisse du traffic.
  - On peut envoyer un mail en cas d'alerte
- Page de stats
  - Création de graphiques en fonction de critères précis.

    - Machine/ IP destination / Ports

    - Interfaces entrée / sortie

    - Et d'autres…

UTILISATION DE NFSEN

- Visualiser le traffic par AS src/dst, port/IP src/dst, et bien d'autres options
- Identification des protocoles et IP les plus actifs
- C'est un outil qui complémente Cacti pour voir plus de détail sur le trafic
- On peut prendre des décisions à partir des information telles que:
  - Beaucoup de trafic SMTP-> Diminuer le trafic SMTP
  - Des machines envoient beaucoup du SPAM -> Intervenir directement aux machines concernées.