TP Supervision réseau

NetFlow

Jean-Marc Têtu

Membres du service en charge de l'administration du réseau d'un établissement d'enseignement supérieur, vous devez configurer et utiliser les outils qui permettront de superviser la connexion à Internet.

Cette supervision doit relever et stocker les informations permettant :

1. de déterminer à partir de l'IP d'un serveur externe (à votre réseau) et d'une date (année,mois,jour,heure,minute) si l'une des machines internes y a eu accès, et si oui, laquelle.
2. de Détecter les excès d'utilisation de bande passante par l'une des machines connectées à votre réseau (vous pensez bien entendu aux élèves).
3. de déterminer à partir d'un numéro de port (TCP ou UDP) spécifique, si une ou plusieurs machines de votre réseau sont infectées par un (très pernicieux) virus.

Par acquis de conscience, vous allez vérifier l'exactitude des informations remontées avec l'outil de base de tout bon administrateur de réseau : wireshark.

Utilisation de Netflow

Définition :

Le protocole Netflow de Cisco permet de comptabiliser sous un seul « flow » toutes les trames partageant des caractéristiques communes (Ip source et destination, ports, etc…) et qui se suivent sans interruption.
En conséquence , un intervalle > 15 secondes (valeur par défaut) entre deux trames ayant par ailleurs les mêmes caractéristiques, fera apparaitre deux flows et non un seul.

Extrait de la RFC 3954

A flow is defined as a unidirectional sequence of packets with some common properties that pass through a network device. These collected flows are exported to an external device, the NetFlow collector. Network flows are highly granular; for example, flow records include details such as IP addresses, packet and byte counts, timestamps, Type of Service (ToS), application ports, input and output interfaces, etc

exemple d'une sortie Netflow

Date flow start	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Packets	Bytes	Flows
2011-09-16 13:48:55.225	50.240	UDP	192.108.116.130:60217	78.45.237.35:1028	6	899	1
2011-09-16 13:49:01.113	44.320	TCP	192.108.116.130:55579	82.96.64.4:6667	11	601	1
2011-09-16 13:49:01.145	44.288	TCP	82.96.64.4:6667	192.108.116.130:55579	10	1326	1
2011-09-16 13:49:19.417	25.792	TCP	192.108.116.129:57983	74.125.230.91:80	16	6713	1
2011-09-16 13:49:19.449	25.760	TCP	192.108.116.129:58023	74.125.230.91:80	8	2732	1

Utilisation de Netflow

Configuration d'un routeur

1. Définir un serveur de « collecte » : ip flow-export destination *votre_ip* **2056**
2. Activer la collecte sur les interfaces (suivant le sens du trafique):
    a. ip flow ingress
    b. ip flow egress
3. Exemple minimal :

```
ip flow-export destination 10.29.84.2 2056
interface GigabitEthernet0/0/1.807
 ip flow ingress
```

4. Vérifier le fonctionnement :

- show ip cache verbose flow
- show ip flow export

Excercice 1

1. Activez le netflow sur le routeur de façon à collecter les informations en direction de l'exterieur et les envoyer vers votre « serveur »
2. Générez du trafique passant par l'interface du routeur (ping, iperf, etc)
3. Vérifiez son bon fonctionnement par la commande adhoc de l'IOS
4. Vérifiez que vous recevez bien les informations netflow sur votre PC en utilisant wireshark.

Configuration du serveur de « collecte »

1. Nous allons utiliser la suite logicielle (nfdump, nfcapd, nfsen)
    a. Nfcapd : démon qui reçoit les infos venant du routeur et les stocke sous forme de fichier binaire.
    b. Nfdump : utilitaire permettant de lire les fichiers générés par nfcapd.
    c. Nfsen : interface web en php permettant de présenter de manière plus synthétique et interactive les résultats de l'accounting (s'appuie sur nfdump)…

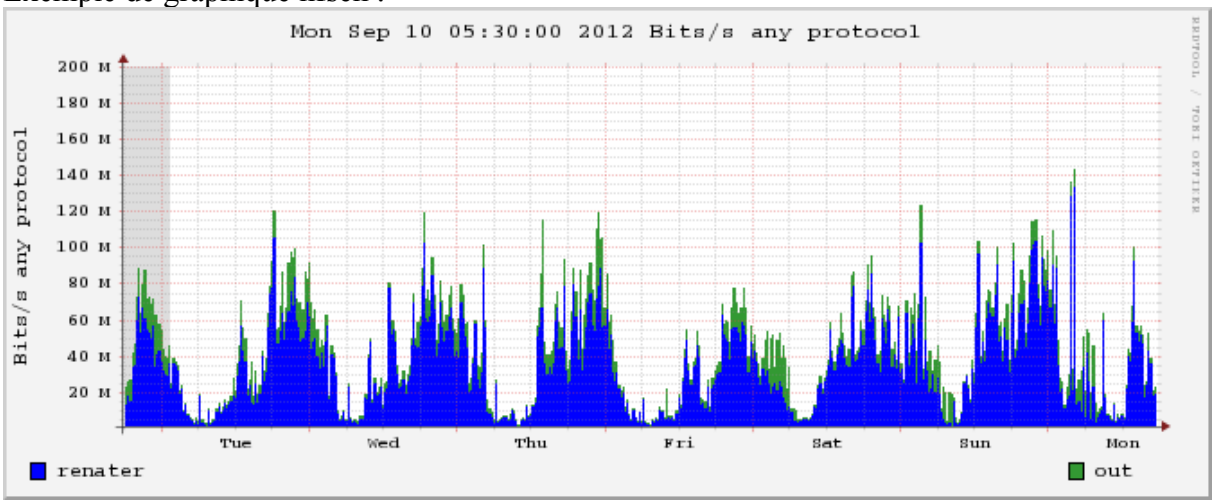
Exemple de commande nfcapd :

```
/u01/app/netflow/nfdump/bin//nfcapd -w -D -I renater -p 2056 -u apache -g apache -B 200000 -S 1 -l /u02/nfsen/profiles-data/live/renater -P /u02/nfsen/var/run/renater.pid
```

Exemple de commande nfdump :

```
/u01/app/netflow/nfdump/bin/nfdump  -c 15 -o fmt:"%in %out %pr %sa %sp %dp   %dir %da %fwd"  -r nfcapd.201109192355 "host 192.108.116.131"
```

Exemple de graphique nfsen :



2. nfcapd peut être lancé sans trop se soucier de la syntaxe exacte de la commande via la confguration de nfsen.

Exercice 2

Vous allez configurer nfsen. L'installation a déjà été réalisée dans /opt.

1. Editez le fichier de configuration et faites prendre en compte vos modifications.
2. « démarrez nfsen »
3. vérifiez que nfcapd est bien lancé.
4. Générez du trafique (ping, requete http…)
5. Vérifier que les fichiers sont bien créés dans le repertoire « profiles-data »
6. Vérifiez que vous voyez bien apparaitre des infos sur l'interface web. (http://localhost/nfsen/)

Exploitation

Exercice 3 : retrouver l'IP d'une machine ayant accédé à un serveur.

1. Affichez la « une » du site : http://www.telecom-bretagne.eu/lexians/
2. Retrouvez directement avec nfdump que vous avec bien accédé à ce serveur
3. Retrouvez avec nfsen la même information.
4. Affichez la « une » du site du monde.fr (ou d'un autre grand quotidien en ligne).
5. Retrouvez la trace de cet accès avec nfsen (syntaxe du filtre à utiliser : dst ip *ip_serveur*)
6. Affichez la « une » de www.telecom-bretagne.eu. Quelles sont les différences avec l'accounting obtenu avec le monde et lexians. Quelles conclusions en tirez vous ?
7. Renouvelez l'opération avec wireshark. Quelles sont les différences ? Quelles conclusions en tirez vous ?

Excercice 4 : détecter une pointe de trafique

1. Générez de manière intensive avec « iperf ». Demandez à un autre groupe de lancer un iperf en mode « serveur » et lancez le votre en mode client.
2. Regardez le résultat avec nfsen. La pointe de trafique est elle bien visible ? Combien de flow sont ils recensés ? Peut-on retrouver la vitesse de transfert entre les deux iperf ?
3. refaites la même expérience avec un wireshark ou un tcpdump , mais en sauvegardant le résultat. Comparez la taille de fichier nécessaire avec celui généré par l'accounting netflow. Qu'en concluez vous ?

Excercice 5 : détecter un virus par l'utilisation de ports non conventionnels

1. Avec iperf, vous simulerez un virus causant sur le port tcp « 1666 ».
2. Retrouvez avec nfsen ce trafique et identifiez la machine l'ayant généré (syntaxe du filtre à utiliser : « src port *numero ») *