Groupe de travail Réseau
Request for Comments : 5470
Categorie : Information

Traduction Claude Brière de L'Isle

G. Sadasivan, Rohati Systems
N. Brownlee, CAIDA | University of Auckland
B. Claise, Cisco Systems, Inc.
J. Quittek, NEC
mars 2009

Architecture d'exportation d'informations de flux IP

Statut de ce mémoire
Le présent mémoire apporte des informations pour la communauté de l'Internet. Le présent mémoire ne spécifie aucune sorte de norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le présent mémoire définit l'architecture de l'exportation d'informations de flux IP (IPFIX, *IP Flow Information eXport*) pour la surveillance sélective des flux IP, et pour l'exportation des informations de flux IP mesurés d'un appareil IPFIX à un collecteur.

Table des matières

1. Introduction

Plusieurs applications, par exemple, la comptabilité fondée sur l'usage, le profilage du trafic, l'ingénierie du trafic, la détection d'attaque/intrusion, la surveillance de la qualité de service (QS) qui exigent des mesures du trafic IP fondées sur le flux. Il est donc important d'avoir une façon standard d'exporter les informations relatives aux flux IP. Le présent document définit une architecture pour la surveillance, la mesure, et l'exportation des flux de trafic IP. Il donne une description générale des composants clés d'un appareil IPFIX et de leurs fonctions.

1.1 Portée du document

Le présent document définit l'architecture pour IPFIX. Ses principaux objectifs sont de :

- Décrire les composants clés de l'architecture IPFIX, consistant en (au moins) des appareils et des collecteurs IPFIX qui communiquent en utilisant le protocole IPFIX.
- Définir les exigences architecturales de IPFIX, par exemple, récupération, sécurité, etc.
- Décrire les caractéristiques du protocole IPFIX.

1.2 Vue d'ensemble des documents IPFIX

Le protocole IPFIX fournit aux administrateurs de réseau l'accès aux informations de flux IP. Le présent document spécifie l'architecture pour l'exportation des informations de flux IP mesurées d'un processus d'exportation IPFIX à un processus collecteur, selon les exigences définies dans la [RFC3917]. Le document de protocole IPFIX, la [RFC5101], spécifie comment les enregistrements et gabarits de données IPFIX sont portés via un protocole de transport qui tient compte de l'encombrement, d'un processus d'exportation IPFIX au processus de collecte IPFIX. IPFIX a une description formelle des éléments d'information IPFIX (des champs) de leur nom, type, et des informations de sémantique supplémentaires, comme spécifié dans la [RFC5102]. Finalement, la [RFC5472] décrit les types d'applications qui peuvent utiliser le protocole IPFIX et comment elles peuvent utiliser les informations fournies. De plus, elle montre comment le cadre de IPFIX se rapporte aux autres architectures et cadres.

Noter que le système IPFIX ne fournit pas la configuration à distance d'un appareil IPFIX. Les mises en œuvre doivent plutôt fournir une façon efficace de configurer leurs appareils IPFIX.

2. Terminologie

Les définitions des termes IPFIX de base tels que flux de trafic IP, processus d'exportation, processus de collecte, point d'observation, etc., sont sémantiquement identiques à celles qui se trouvent dans le document des exigences pour IPFIX

[RFC3917]. Certains des termes ont été étendus pour plus de clarté dans la définition du protocole. Des définitions supplémentaires requises pour l'architecture ont aussi été ajoutées. Pour les termes qui sont définis ici et dans la [RFC5101], les définitions des deux documents sont équivalentes.

* Point d'observation : un point d'observation est une situation dans le réseau où les paquets IP peuvent être observés. Des exemples incluent une ligne à laquelle une sonde est rattachée, un support partagé, comme un LAN fondé sur Ethernet, un seul accès d'un routeur, ou un ensemble d'interfaces (physiques ou logiques) d'un routeur. Noter que chaque point d'observation est associé à un domaine d'observation (défini ci-dessous) et qu'un point d'observation peut être un sur-ensemble de plusieurs points d'observation. Par exemple, un point d'observation peut être une carte de ligne entière. Cela serait le sur-ensemble des points d'observation individuels aux interfaces de la carte de ligne.

* Domaine d'observation : un domaine d'observation est le plus grand ensemble de points d'observation pour lequel des informations de flux peuvent être agrégées par un processus de mesure. Par exemple, une carte de ligne de routeur peut être un domaine d'observation si elle est composée de plusieurs interfaces, dont chacune est un point d'observation. Dans le message IPFIX qu'il génère, le domaine d'observation inclut son identifiant de domaine d'observation, qui est unique par processus d'exportation. De cette façon, le processus collecteur peut identifier le domaine d'observation spécifique à partir de l'exportateur qui envoie les messages IPFIX. Chaque point d'observation est associé à un domaine d'observation. Il est recommandé que les identifiants de domaine d'observation soient aussi uniques par appareil IPFIX.

* Flux de trafic IP ou flux : il y a plusieurs définitions du terme de "flux" qui sont utilisées par la communauté de l'Internet. Dans le contexte de IPFIX, on utilise la définition suivante : un flux est défini comme un ensemble de paquets IP passant à un point d'observation dans le réseau durant un certain intervalle de temps. Tous les paquets appartenant à un flux particulier ont un ensemble de propriétés communes. Chaque propriété est définie comme le résultat de l'application d'une fonction aux valeurs de :
  1. un ou plusieurs champs d'en-tête de paquet (par exemple, adresse IP de destination) champs d'en-tête de transport (par exemple, numéro d'accès de destination) ou champs d'en-tête d'application (par exemple, champs d'en-tête RTP [RFC3550]).
  2. une ou plusieurs caractéristiques du paquet lui-même (par exemple, nombre d'étiquettes MPLS)
  3. un ou plusieurs champs dérivés du traitement de paquet (par exemple, adresse IP du prochain bond, interface de sortie)

  Un paquet est défini comme appartenant à un flux si il satisfait complètement toutes les propriétés définies du flux.
  Cette définition couvre la gamme d'un flux contenant tous les paquets observés à une interface du réseau à un flux consistant juste en un seul paquet entre deux applications. Elle inclut des paquets choisis par un mécanisme d'échantillonnage.

* Clé de flux : chacun des champs qui :
  1. appartient à l'en-tête de paquet (par exemple, adresse IP de destination),
  2. est une propriété du paquet lui-même (par exemple, longueur du paquet),
  3. est déduit du traitement de paquet (par exemple, numéro de système autonome (AS)), et
  4. est utilisé pour définir un flux,

  est appelé une clé de flux.

* Enregistrement de flux : un enregistrement de flux contient des informations sur un flux spécifique qui a été observé à un point d'observation. Un enregistrement de flux contient les propriétés mesurées du flux (par exemple, le nombre total d'octets pour tous les paquets du flux) et généralement les propriétés caractéristiques du flux (par exemple, adresse IP de source).

* Processus de mesure : le processus de mesure génère des enregistrements de flux. Les entrées au processus sont les en-têtes de paquet et les caractéristiques observées à un point d'observation, et le traitement de paquet au point d'observation (par exemple, l'interface de sortie choisie). Le processus de mesure consiste en un ensemble de fonctions qui incluent la capture des en-têtes de paquet, l'horodatage, l'échantillonnage, la classification, et la maintenance des enregistrements de flux. La maintenance des enregistrements de flux peut inclure de créer de nouveaux enregistrements, de mettre à jour ceux existants, de calculer les statistiques de flux, de déduire d'autres propriétés de flux, de détecter l'expiration des flux, de passer les enregistrements de flux au processus d'exportation, et de supprimer les enregistrements de flux.

* Processus d'exportation : le processus d'exportation envoie des enregistrements de flux à un ou plusieurs processus de collecte. Les enregistrements de flux sont générés par un ou plusieurs processus de mesure.

* Exportateur : appareil qui héberge un ou plusieurs processus d'exportation.

* Appareil IPFIX : un appareil IPFIX héberge au moins un processus d'exportation. Il peut héberger d'autres processus d'exportation et des nombres arbitraires de points d'observation et de processus de mesure.

* Processus de collecte : un processus de collecte reçoit des enregistrements de flux d'un ou plusieurs processus d'exportation. Le processus de collecte pourrait traiter ou mémoriser les enregistrements de flux reçus, mais de telles actions sortent du domaine d'application du présent document.

* Collecteur : appareil qui héberge un ou plusieurs processus de collecte.

* Gabarit : séquence ordonnée de paires de <type, longueur> utilisées pour spécifier complètement la structure et la sémantique d'un ensemble particulier d'informations qui doivent être communiquées d'un appareil IPFIX à un collecteur. Chaque gabarit est identifiable de façon univoque au moyen d'un identifiant de gabarit.

* Informations de contrôle, flux de données : les informations qui doivent être exportées de l'appareil IPFIX peuvent être classés dans les catégories suivantes :
  Informations de contrôle : cela inclut la définition du flux, les critères de choix des paquets au sein du flux envoyé par le processus d'exportation, et les gabarits qui décrivent les données à exporter. Les informations de contrôle portent toutes les informations nécessaires aux points d'extrémité pour comprendre le protocole IPFIX, et spécifiquement pour que le collecteur comprenne et interprète les données envoyés par l'exportateur envoyeur.
  Flux de données : cela inclut les enregistrements de flux portant les valeurs de champs pour les divers flux observés à chaque point d'observation.

* Message IPFIX : un message IPFIX est un message généré au processus d'exportation qui porte les enregistrements IPFIX de son processus d'exportation et dont la destination est un processus de collecte. Un message IPFIX est encapsulé à la couche transport.

* Élément d'information : un élément d'information est une description de protocole indépendante du codage d'un attribut qui peut apparaître dans un enregistrement IPFIX. Le modèle d'information IPFIX [RFC5102], définit l'ensemble de base des éléments d'information pour IPFIX. Le type associé à un élément d'information indique les contraintes sur ce qu'il peut contenir et aussi détermine les mécanismes de codage valides à utiliser dans IPFIX.

3. Exemples de flux

Des exemples de flux sont donnés ci-dessous. Dans les exemples IPv4, on utilise des adresses d'interface dans trois différents sous réseaux de 26 bits (/26). Dans les exemples IPv6, on utilise "mac addr-nn" dans les 64 bits de moindre poids pour indiquer l'adresse de commande d'accès au support (MAC, *Media Access Control*) IEEE de l'interface nn de l'hôte.

Exemple 1 : les clés de flux définissent les différents champs qui distinguent les flux. La combinaison différente de leurs valeurs de champs crée des flux uniques. Si des {adresse IP de source, adresse IP de destination, DSCP} sont des clés de flux, alors toutes sont des flux différents :

1. {192.0.2.1, 192.0.2.65, 4}
2. {192.0.2.23, 192.0.2.67, 4}
3. {192.0.2.23, 192.0.2.67, 2}
4. {192.0.2.129, 192.0.2.67, 4}

5. {2001:DB8::0:mac-addr-01, 2001:DB8::1:mac-addr-11, 4}
6. {2001:DB8::0:mac-addr-02, 2001:DB8::1:mac-addr-13, 4}
7. {2001:DB8::0:mac-addr-02, 2001:DB8::1:mac-addr-13, 2}
8. {2001:DB8::2:mac-addr-21, 2001:DB8::1:mac-addr-13, 4}

Exemple 2 : une fonction de gabarit peut être appliquée à tous les paquets qui passent par un point d'observation, afin d'agréger certaines valeurs. Cela pourrait être fait en définissant l'ensemble de clés de flux comme des {adresse IP de source, adresse IP de destination, DSCP}comme dans l'exemple 1 ci-dessus, et en appliquant les fonctions qui dessinent les adresses IP de source et de destination (6 bits de moindre poids pour IPv4, 64 bits pour IPv6). Les huit flux de l'exemple 1 seraient maintenant agrégés en six flux en fusionnant les flux 1+2 et 5+6 :

1. {192.0.2.0/26, 192.0.2.64/26, 4}
2. {192.0.2.0/26, 192.0.2.64/26, 2}

3. {192.0.2.128/26, 192.0.2.64/26, 4}

4. {2001:DB8::0/64, 2001:DB8::1/64, 4}
5. {2001:DB8::0/64, 2001:DB8::1/64, 2}
6. {2001:DB8::2/64, 2001:DB8::1/64, 4}

Exemple 3 : un filtre défini par des valeurs de clé de flux peut être appliqué à tous les paquets qui passent par le point d'observation, afin de choisir seulement certains flux. Le filtre est défini en choisissant des valeurs fixes pour des clés spécifiques provenant du paquet.

Tous les paquets qui vont d'un réseau de consommateur 192.0.2.0/26 à un autre réseau de consommateur 192.0.2.64/26 avec une valeur de DSCP de 4 définissent un flux. Toutes les autres combinaisons ne définissent pas de flux et sont ne sont pas prises en compte. Les trois flux de l'exemple 2 seraient alors réduits à un flux en filtrant les flux 2 et 3, laissant seulement le flux 1, {192.0.2.0/26, 192.0.2.64/26, 4}.

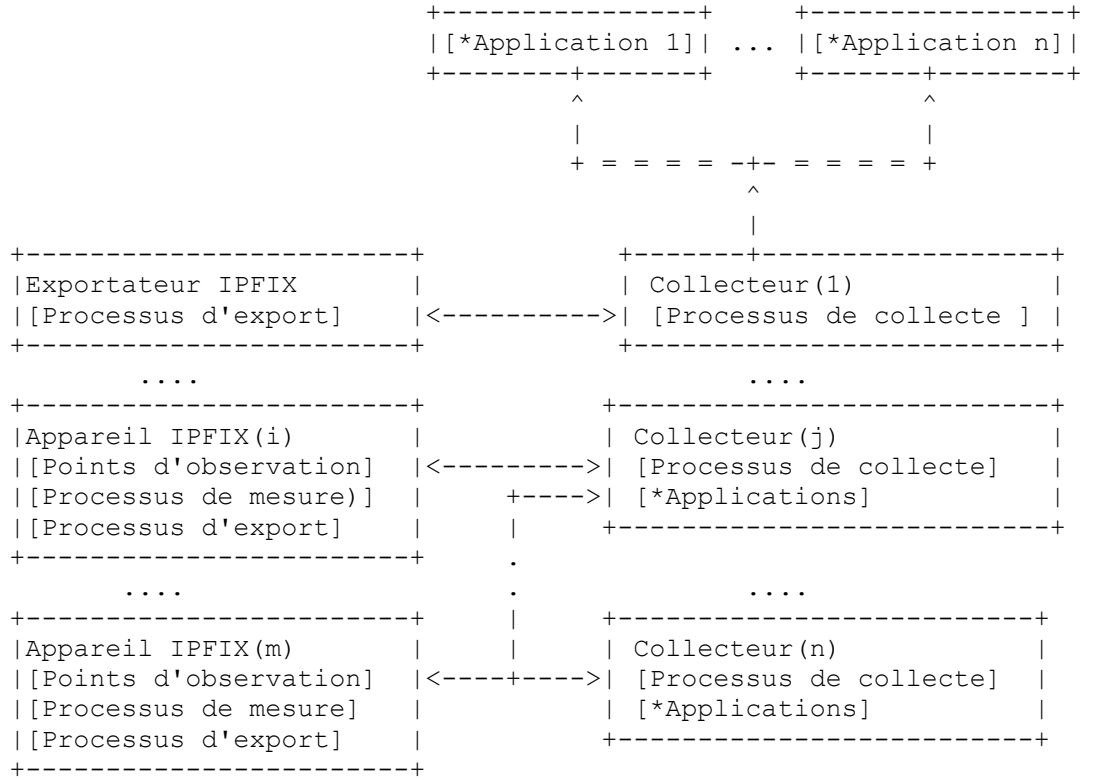
De même, pour les paquets IPv6 dans les exemples ci-dessus, on pourrait filtrer les flux 5 et 6 pour laisser le flux 4.

Les exemples ci-dessus peuvent être vus comme une fonction F() prenant en entrée {adresse IP de source, adresse IP de destination, DSCP}. La fonction choisit seulement les paquets qui satisfont les trois conditions suivantes :
1. en occultant les 6 bits de moindre poids de l'adresse IP de source, correspondent à 192.0.2.0 ;
2. en occultant les 6 bits de moindre poids de l'adresse IP de destination, correspondent à 192.0.2.64 ;
3. acceptent seulement la valeur de DSCP de 4.

Selon les valeurs de {adresse IP de source, adresse IP de destination, DSCP} des différents paquets observés, la fonction de processus de mesure F() va choisir/filtrer/agréger différents ensembles de paquets, qui vont créer différents flux. Par exemple, pour diverses combinaisons de valeurs de {adresse IP de source, adresse IP de destination, DSCP}, F(adresse IP de source, adresse IP de destination, DSCP) va résulter en la définition d'un ou plusieurs flux.

4. Modèle de référence IPFIX

La figure ci-dessous montre le modèle de référence pour IPFIX. Cette figure couvre les divers scénarios possibles qui peuvent exister dans un système IPFIX.



Les divers composants fonctionnels sont indiqués entre des crochets []. Les composants fonctionnels entre des [*] ne font pas partie de l'architecture IPFIX. Les interfaces montrées par "<----->" sont définies par l'architecture IPFIX, mais celles montrées par "<= = = =>" ne le sont pas.

Figure 1 : Modèle de référence IPFIX

La figure ci-dessous montre un appareil IPFIX typique où les composants IPFIX sont montrés dans des boîtes rectangulaires.

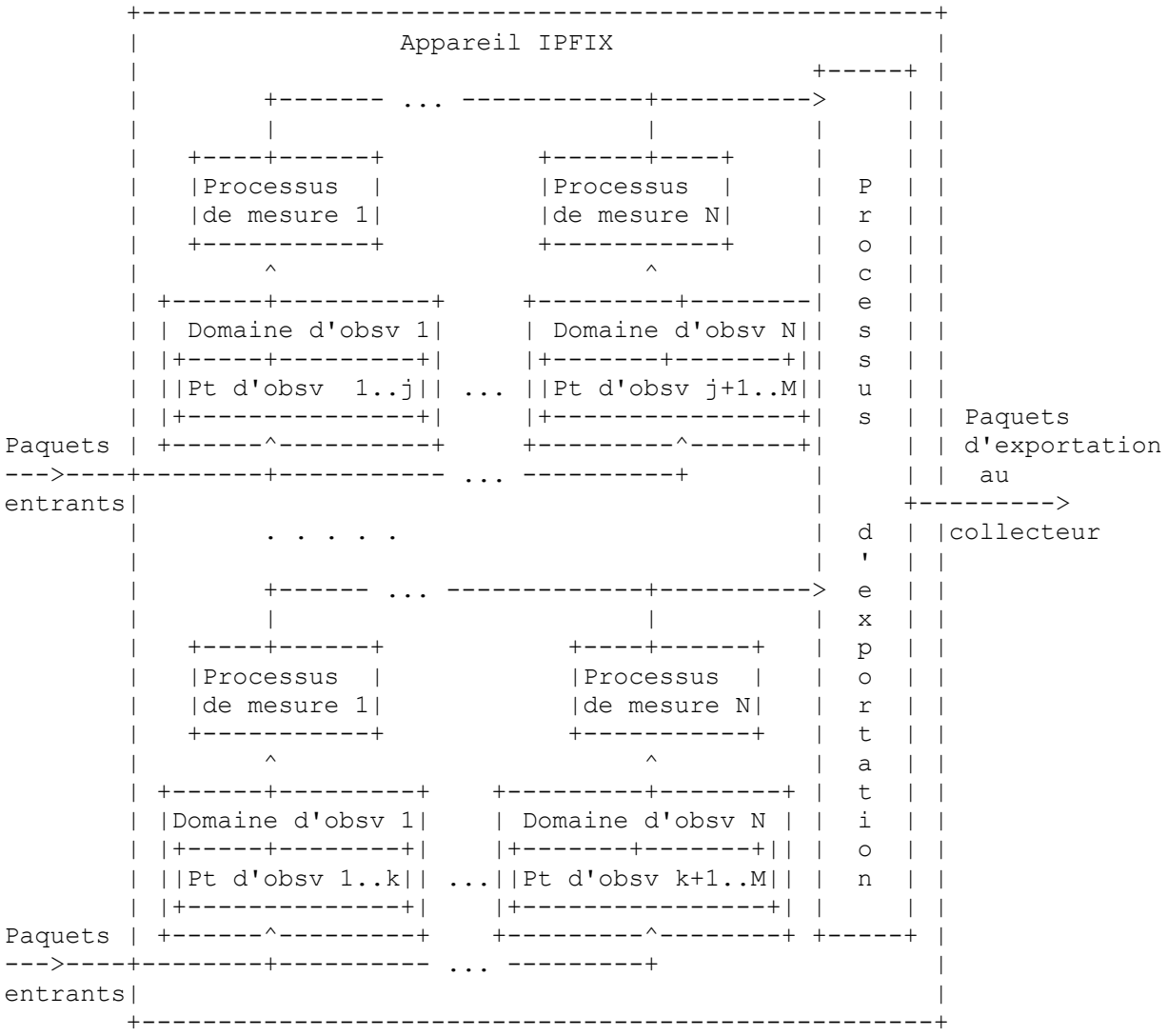


Figure 2 : Appareil IPFIX

5. Blocs IPFIX fonctionnels et logiques

5.1 Processus de mesure

Chaque point d'observation dans un appareil IPFIX, participant aux mesures de flux, doit être associé à au moins un processus de mesure. Chaque paquet arrivant à un point d'observation entre dans chaque processus de mesure associé au point d'observation. En gros, chaque processus de mesure observe les paquets qui passent par un point d'observation, fait l'horodatage, et classe les paquets dans le ou les flux sur la base des critères de choix.

Le processus de mesure est un bloc fonctionnel qui gère tous les flux générés à partir d'un domaine d'observation. Les fonctions typiques d'un processus de mesure peuvent inclure :

- de tenir les bases de dnnées de tous les enregistrements de flux provenant d'un domaine d'observation. Cela inclut de créer de nouveaux enregistrements de flux, de mettre à jour ceux existants, de calculer les statistiques d'enregistrements de flux, de déduire d'autres propriétés de flux, et d'ajouter des informations non spécifiques du flux sur la base du traitement de paquet (dans certains cas, des champs comme les numéros d'AS, l'état du routeur, etc.)

- De tenir des statistiques sur le processus de mesure lui-même, comme les enregistrements de flux générés, les paquets observés, etc.

5.1.1 Expiration de flux

Un flux est considéré avoir expiré dans les conditions suivantes :

1. Si aucun paquet appartenant au flux n'a été observé pendant un certain temps. Ce temps devrait être configurable au processus de mesure, avec une valeur minimum de 0 seconde pour une expiration immédiate. Noter qu'une temporisation de zéro va rapporter un flux comme une séquence de flux d'un seul paquet.

2. Si l'appareil IPFIX rencontre des contraintes de ressources, un flux peut expirer prématurément (par exemple, manque de mémoire pour les enregistrements de flux).

3. Pour les flux de longue durée, le processus de mesure devrait faire expirer le flux sur une base régulière ou sur la base d'une politique d'expiration. Cette périodicité ou politique d'expiration devrait être configurable au processus de mesure. Quand un flux de longue durée expire, son enregistrement de flux peut quand même être maintenu par le processus de mesure afin que le processus de mesure n'ait pas besoin de créer un nouvel enregistrement de flux pour d'autres paquets observés du même flux.

5.1.2 Exportation de flux

Le processus d'exportation décide quand et si exporter un flux expiré. Un flux peut être exporté parce qu'il a expiré pour une des raisons mentionnées au paragraphe 5.1.1, "Expiration de flux". Par exemple, le processus d'exportation exporte une portion des flux expirés toutes les "x" secondes.

Pour les flux de longue durée, le processus d'exportation devrait exporter les enregistrements de flux sur une base régulière ou sur la base d'une politique d'exportation. Cette périodicité ou politique d'exportation devrait être configurable au processus d'exportation.

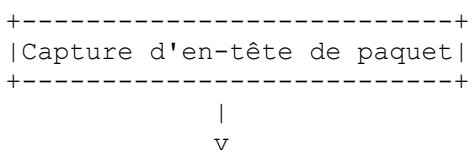
5.2 Point d'observation

Un enregistrement de flux peut être mieux analysé si le point d'observation à partir duquel il a été mesuré est connu. À ce titre, il est recommandé que les appareils IPFIX envoient ces informations aux collecteurs. Dans les cas où il y a un seul point d'observation ou quand les informations du point d'observation ne sont pas pertinentes, le processus de mesure peut choisir de ne pas ajouter les informations du point d'observation aux enregistrements de flux.

5.3 Critère de choix des paquets

Un processus de mesure peut définir des règles afin que seuls certains paquets au sein d'un flux entrant de paquets soient choisis pour les mesures à un point d'observation. Cela peut être fait par une des deux méthodes définies ci-dessous ou par une combinaison des deux, dans n'importe quel ordre. Une combinaison de chacune de ces méthodes peut être adoptée pour choisir les paquets, c'est-à-dire, on peut définir un ensemble de méthodes {F1, S1, F2, S2, S3} exécuté dans une séquence spécifiée à un point d'observation pour choisir des flux particuliers.

La figure ci-dessous montre les opérations qui peuvent être appliquées au titre d'un processus de mesure normal.



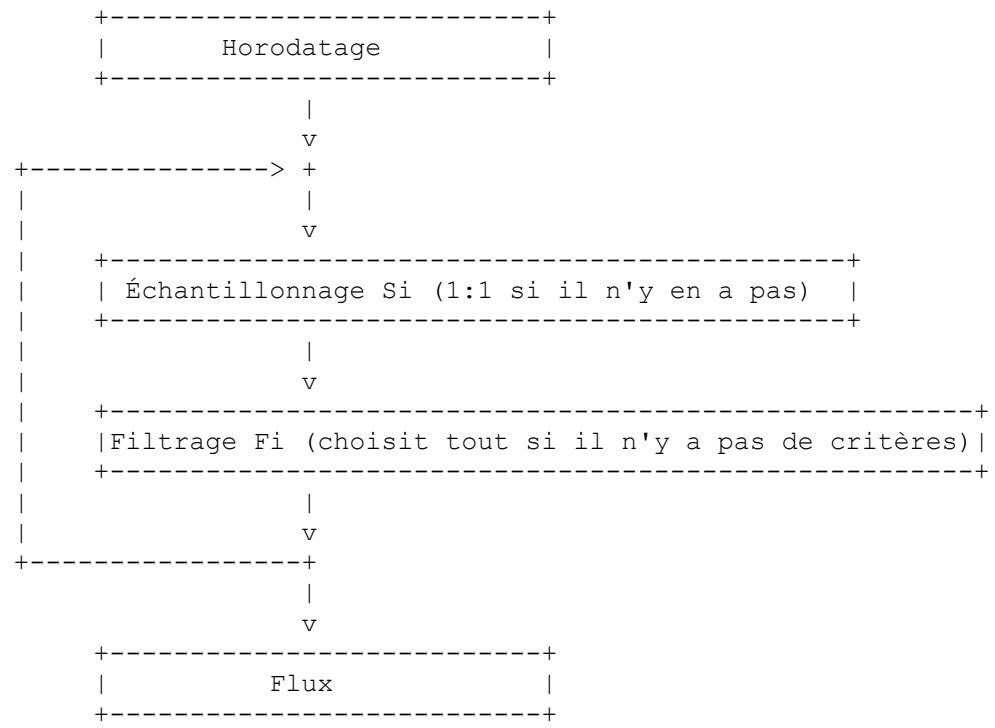


Figure 3 : Critères de choix des paquets

Noter que des paquets pourraient être choisis avant ou après tout traitement IP, c'est-à-dire, avant toute validation de somme de contrôle, filtrage IP, etc., ou après une ou plusieurs de ces étapes. Cela a un impact sur la sorte de trafic (ou conditions d'erreur) que IPFIX peut observer. Il est recommandé que les paquets soient choisis après la vérification de leur somme de contrôle.

5.3.1 Fonctions d'échantillonnage, Si

Une fonction d'échantillonnage détermine quels paquets au sein d'un flux de paquets entrants sont choisis pour les mesures, c'est-à-dire, les paquets qui satisfont les critères d'échantillonnage pour ce processus de mesure.

Exemple : échantillonner chaque 100ième paquet reçu à un point d'observation.

Choisir tous les paquets est un cas particulier où le taux d'échantillonnage est 1:1.

5.3.2 Fonctions de filtrage, Fi

Une fonction de filtrage choisit seulement les paquets entrants qui satisfont une fonction sur des champs définis par les champs d'en-tête de paquet, les champs obtenus pendant le traitement du paquet, ou des propriétés du paquet lui-même.

Exemple :
Gabarit/correspondance sur les champs que définit un filtre. Un filtre pourrait être défini comme {Protocole == TCP, Accès de destination < 1024}.

Plusieurs de ces filtres pourraient être utilisés dans n'importe quel ordre pour choisir les paquets. Noter que les paquets choisis par des (une séquence de) fonctions de filtre peuvent ensuite être classés par d'autres fonctions de filtre, c'est-à-dire, les paquets choisis peuvent appartenir à plusieurs flux, dont certains ou tous sont exportés.

5.4 Domaine d'observation

Le domaine d'observation est un bloc logique qui présente une seule identité pour un groupe de points d'observation au sein d'un appareil IPFIX. Chaque paire de {point d'observation, processus de mesure} appartient à un seul domaine d'observation. Un appareil IPFIX pourrait avoir plusieurs domaines d'observation, dont chacun a en lui un sous ensemble de

l'ensemble total des points d'observation. Chaque domaine d'observation doit porter un identifiant unique dans le contexte d'un appareil IPFIX. Noter que dans le cas de plusieurs domaines d'observation, un identifiant unique par domaine d'observation doit être transmis comme un paramètre à la fonction d'exportation. Cet identifiant unique est appelé l'identifiant de domaine d'observation IPFIX.

5.5 Processus d'exportation

Le processus d'exportation est le bloc fonctionnel qui envoie les données à un ou plusieurs collecteurs IPFIX en utilisant le protocole IPFIX. D'un côté, le processus d'exportation s'interface avec le ou les processus de mesure pour obtenir les enregistrements de flux; tandis que de l'autre côté, il parle à un processus de collecte sur le ou les collecteurs.

Des règles supplémentaires peuvent être définies au sein d'un domaine d'observation afin que seuls certains enregistrements de flux soient exportés. Cela peut être fait par Si ou Fi, ou une de leurs combinaison, comme décrit au paragraphe 5.3, "Critères de choix des paquets".

Exemple : seuls les enregistrements de flux qui satisfont les critères de choix suivants sont exportés :
1. Tous les enregistrements de flux dont l'adresse IP de destination satisfait {192.0.33.5}.
2. Tous les autres (c'est-à-dire, le taux d'échantillonnage 1 sur 2) enregistrements de flux dont l'adresse de destination IP satisfait {192.0.11.30}.

5.6 Processus de collecte

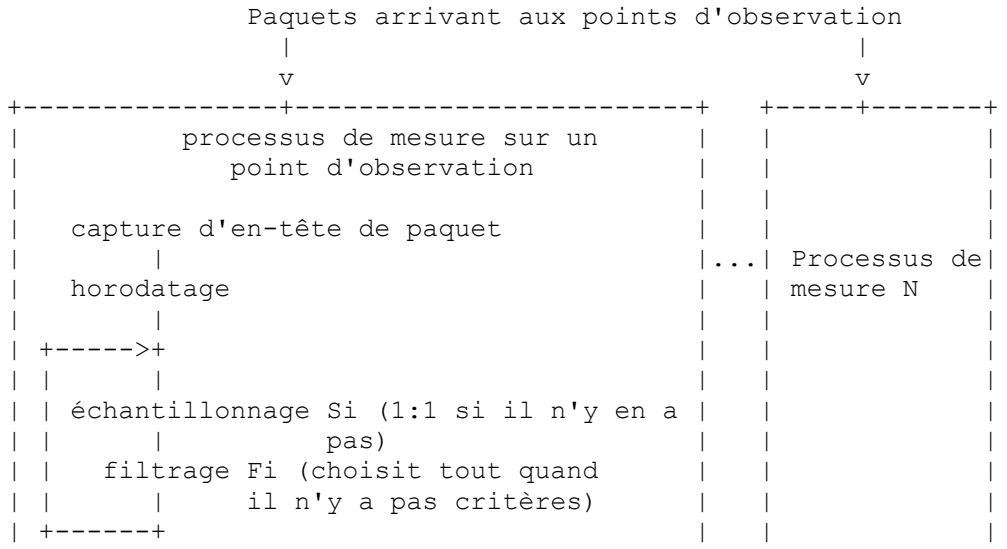
Les processus de collecte utilisent l'identifiant de gabarit de l'enregistrement de flux pour interpréter les éléments d'information de cet enregistrement de flux. Pour permettre cela, un exportateur IPFIX doit s'assurer qu'un collecteur IPFIX connaît l'identifiant de gabarit pour chaque enregistrement de flux entrant. Pour interpréter les enregistrements de flux entrants, un collecteur IPFIX peut aussi devoir connaître la fonction F() qui a été utilisée par le processus de mesure pour chaque flux.

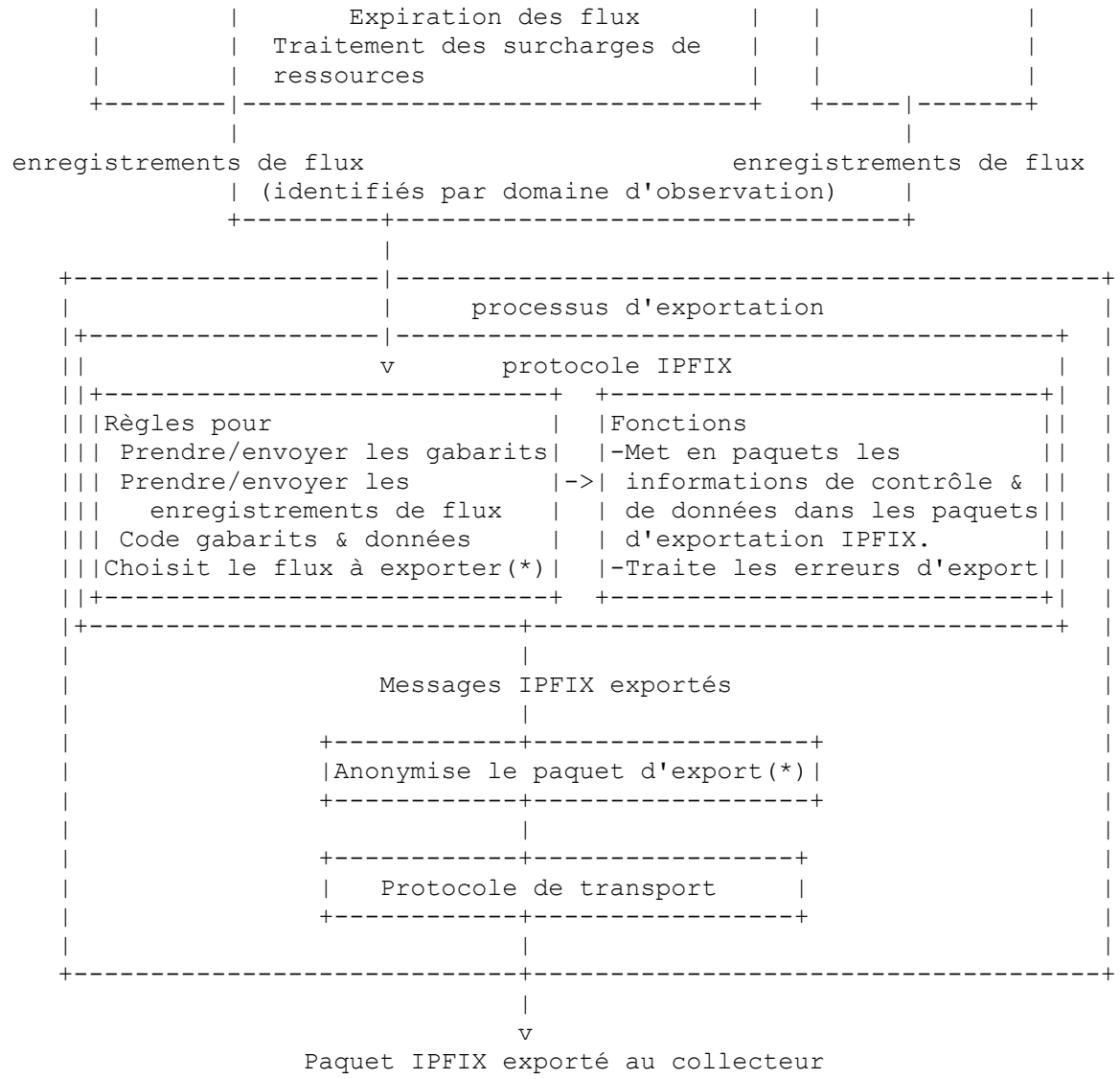
Les fonctions du processus de collecte doivent inclure :
- o d'identifier, accepter, et décoder les messages IPFIX provenant de différentes paires de <processus d'exportation, domaine d'observation> ;
- o mémoriser les informations de contrôle et enregistrements de flux reçus d'un appareil IPFIX.

À haut niveau, le processus de collecte :
1. reçoit et mémorise les informations de contrôle ;
2. décode et mémorise les enregistrements de flux en utilisant les informations de contrôle.

5.7 Résumé

La figure ci-dessous montre les fonctions effectuées à la suite par les divers blocs fonctionnels dans un appareil IPFIX.





(*) indique que le bloc est facultatif.

Figure 4 : Blocs fonctionnels d'appareil IPFIX

6. Vue d'ensemble du protocole IPFIX

Un appareil IPFIX consiste en un ensemble de processus coopérants qui mettent en œuvre les blocs fonctionnels décrits au paragraphe précédent. Autrement, un appareil IPFIX peut être vu simplement comme une entité du réseau qui met en œuvre le protocole IPFIX. À l'appareil IPFIX, la fonction du protocole réside dans le processus d'exportation. Le processus d'exportation IPFIX obtient les enregistrements de flux d'un processus de mesure, et les envoie aux collecteurs.

À haut niveau, un appareil IPFIX effectue les tâches suivantes :
1. Code les informations de contrôle dans des gabarits.
2. Code les paquets observés aux points d'observation en enregistrements de flux.
3. Met en paquets les gabarits et enregistrements de flux choisis dans des messages IPFIX.
4. Envoie des messages IPFIX au collecteur.

Le protocole IPFIX communique les informations provenant d'un exportateur IPFIX à un collecteur IPFIX. Ces informations incluent non seulement les enregistrements de flux, mais aussi des informations sur le processus de mesure. De telles informations (appelées des informations de contrôle) incluent des détails des champs de données dans les enregistrements de flux. Elles peuvent aussi inclure des statistiques provenant du processus de mesure, comme le nombre

de paquets perdus (c'est-à-dire, non mesurés).

Pour les détails du protocole IPFIX, voir la [RFC5101].

6.1 Vue d'ensemble du modèle d'information

Le protocole d'exportation de flux IP (IPFIX, *IP Flow Information eXport*) sert à transmettre les informations relatives au trafic IP mesuré sur l'Internet. La spécification du protocole dans la [RFC5101] définit comment les éléments d'information sont transmis. Pour les éléments d'information, il spécifie le codage d'un ensemble de types de données de base. Cependant, la liste des champs qui peuvent être transmis par le protocole, comme les attributs du flux (adresse IP de source, nombre de paquets, etc.) et les informations sur les processus de mesure et d'exportation (point d'observation de paquets, taux d'échantillonnage, intervalle de temporisation de flux, etc.) ne sont pas spécifiées dans la [RFC5101]. Elles sont définies dans le modèle d'information IPFIX de la [RFC5102].

Le modèle d'information donne une description complète des propriétés de chaque élément d'information IPFIX. Il le fait en spécifiant chaque nom d'élément, type de champ, type de données, etc., et en fournissant une description de chaque élément. Les descriptions d'éléments donnent la sémantique de l'élément, c'est-à-dire, elles disent comment il est déduit d'un flux ou d'autres informations disponibles dans un appareil IPFIX.

6.2 Enregistrements de flux

Les règles suivantes donnent des lignes directrices à suivre pour le codage des informations d'enregistrements de flux :

Un enregistrement de flux contient assez d'informations pour que le processus de collecte puisse identifier les <informations de contrôle par flux, informations de contrôle de configuration> correspondantes.

Le processus d'exportation code un élément d'information donné (comme spécifié dans la [RFC5102]) sur la base des normes de codage prescrites par la [RFC5101].

6.3 Informations de contrôle

Les règles suivantes donnent des lignes directrices à suivre pour le codage des informations de contrôle :

- Les informations de contrôle par flux devraient être codées de telle façon que le processus de collecte puisse capturer la structure et la sémantique des données de flux correspondantes pour chaque enregistrement de flux exporté par l'appareil IPFIX.

- Les informations de contrôle de configuration sont convoyées à un collecteur afin que son processus de collecte puisse capturer la structure et la sémantique des données de configuration correspondantes. Les données de configuration, qui sont aussi des informations de contrôle, devraient porter des informations supplémentaires sur le domaine d'observation au sein duquel la configuration prend effet.

Par exemple, l'échantillonnage utilisant le même algorithme d'échantillonnage, disons un paquet sur cent, est configuré sur deux points d'observation, O1 et O2. La configuration peut dans ce cas être codée comme {ID, points d'observation (O1,O2), algorithme d'échantillonnage, intervalle (1 sur 100)}, où ID est l'identifiant du domaine d'observation pour le domaine contenant O1 et O2. L'identifiant de domaine d'observation identifie de façon univoque cette configuration, et doit être envoyé dans les enregistrements de flux afin d'être capable de correspondre aux bonnes informations de contrôle de configuration.

Les informations de contrôle sont utilisées par le processus de collecte pour :
- décoder et interpréter les enregistrements de flux ;
- comprendre l'état du processus d'exportation.

Envoyer les informations de contrôle à partir du processus d'exportation en temps utile et de manière fiable est critique pour le bon fonctionnement du processus de collecte IPFIX. Les approches suivantes peuvent être suivies pour l'exportation des informations de contrôle :

1. Envoyer toutes les informations de contrôle relevant des enregistrements de flux avant d'envoyer les enregistrements de flux eux-mêmes. Cela inclut tout changement incrémentaire de la définition des enregistrements de flux.

2. Notifier, presque en temps réel, l'état de l'appareil IPFIX au processus de collecte. Cela inclut tous les changements tels qu'un changement de configuration qui affecte le comportement de flux, les changements aux ressources du processus d'exportation qui altèrent les taux d'exportation, etc., dont le collecteur doit avoir connaissance.

3. Comme il est vital qu'un processus de collecte conserve une connaissance précise de l'état de l'exportateur, l'exportation des informations de contrôle devrait être faite de telle façon qu'elles atteignent fiablement le collecteur. Une façon de réaliser cela est d'envoyer les informations de contrôle sur un transport fiable.

6.4 Responsabilité des rapports

De temps en temps, un appareil IPFIX peut n'être pas capable d'observer tous les paquets qui atteignent un de ses points d'observation. Cela pourrait arriver si un processus de mesure se trouve temporairement à court de ressources. Par exemple, il pourrait être à court de mémoire tampon de paquets pour l'exportation IPFIX.

Dans de telles situations, l'appareil IPFIX devrait tenter de compter le nombre de pertes de paquets qui se sont produites, et le rapporter à son ou ses collecteurs. Si il n'est pas possible de compter précisément les pertes, par exemple, quand des erreurs de la couche transport (c'est-à-dire, non IPFIX) sont détectées, l'appareil IPFIX devrait rapporter ce fait, et peut-être indiquer la période de temps durant laquelle des paquets pourraient n'avoir pas été observés.

7. Détails du protocole IPFIX

Quand le mandat du groupe de travail IPFIX a été établi, il existait des pratiques courantes dans le domaine de l'exportation de flux, par exemple, NetFlow, la comptabilité fiable courante pour les éléments de réseau (CRANE, *Common Reliable Accounting for Network Element*) le protocole léger d'admission de flux (LFAP, *Light-weight Flow Admission Protocol*) la mesure de flux de trafic en temps réel (RTFM, *Real-time Traffic Flow Measurement*), etc. Le mandat de IPFIX imposait au groupe de travail d'examiner les pratiques existantes, et de choisir celle qui satisfaisait au mieux aux exigences de IPFIX de la [RFC3917]. Des ajouts ou modifications seraient alors faites au protocole choisi pour le faire adhérer exactement à l'architecture IPFIX.

7.1. Protocole IPFIX de base

Le groupe de travail s'est livré à une évaluation extensive des divers protocoles existants disponibles, soupesant le niveau de conformité aux exigences, et choisissant un des candidats comme base du protocole IPFIX. Pour les détails du processus d'évaluation, voir la [RFC3955].

Dans le protocole de base, les enregistrements de flux sont définis par des gabarits, où un gabarit est un ensemble ordonné d'éléments d'information apparaissant dans un enregistrement de flux, avec leurs tailles de champs dans ces enregistrements.

Cette approche donne les avantages suivants :

- En utilisant le mécanisme de gabarit, de nouveaux champs peuvent être ajoutés aux enregistrements de flux IPFIX sans changer la structure du format d'exportation de l'enregistrement.

- Les gabarits qui sont envoyés au processus de collecte portent des informations structurelles sur les champs d'enregistrement de flux exportés. Donc, si le collecteur ne comprend pas la sémantique des nouveaux champs, il peut les ignorer, mais quand même interpréter l'enregistrement de flux.

- Parce que le mécanisme de gabarit est souple, il permet l'exportation des seuls champs requis des flux par le processus de collecte. Cela aide à réduire le volume de données de flux exportées et éventuellement donne des économies de mémoire aux processus d'exportation et de collecte. Envoyer seulement les informations requises peut aussi réduire la charge du réseau.

7.2 Protocole IPFIX sur le processus de collecte

Le processus de collecte est chargé de :

1. Recevoir et décoder les enregistrements de flux provenant des appareils IPFIX.
2. Rapporter les pertes d'enregistrements de flux envoyés au processus de collecte par un processus d'exportation IPFIX.

Les détails complets du protocole IPFIX sont donnés dans la [RFC5101].

7.3 Prise en charge des applications

Les applications qui utilisent les informations collectées par IPFIX peuvent être des sous systèmes de facturation ou de détection d'intrusion, etc. Ces applications peuvent faire partie intégrante du processus de collecte, ou elles peuvent être co-localisées avec le processus de collecte. La façon dont ces applications s'interfacent avec les systèmes IPFIX pour obtenir les informations désirées sort du domaine d'application du présent document.

8. Modèles d'exportation

8.1 Exportation avec une connexion de contrôle fiable

Comme mentionné dans la [RFC3917], un appareil IPFIX doit être capable de transporter ses informations de contrôle et ses flux de données sur un protocole de transport qui évite l'encombrement.

Si le réseau dans lequel l'appareil IPFIX et le processus de collecte sont situés ne garantit pas la fiabilité, au moins les informations de contrôle devraient être exportées sur un transport fiable. Le flux de données peut être exporté sur un protocole de transport fiable ou non fiable.

Les protocoles de transport possibles incluent :
- o SCTP : prend en charge le transport fiable et non fiable.
- o TCP : fournit seulement le transport fiable.
- o UDP : fournit seulement le transport non fiable. Les opérateurs de réseau vont devoir éviter l'encombrement en gardant le trafic dans leur propre domaine administratif. Par exemple, on pourrait utiliser un réseau dédié (ou une liaison Ethernet) pour porter le trafic IPFIX de l'exportateur au collecteur.

8.2 Détection et récupération de défaillance du collecteur

La connexion de transport (dans le cas d'un protocole en mode connexion) est pré-configurée entre l'appareil IPFIX et le collecteur. Le protocole IPFIX ne fournit aucun mécanisme pour configurer les processus d'exportation et de collecte.

Une fois connecté, un collecteur IPFIX reçoit les informations de contrôle et les utilise pour interpréter les enregistrements de flux. L'appareil IPFIX devrait établir un mécanisme de maintien en vie (par exemple, la temporisation de maintien en vie dans le cas de TCP, l'intervalle HEARTBEAT dans le cas de SCTP) à une valeur suffisamment faible pour qu'il puisse rapidement détecter une défaillance du collecteur. Noter cependant que des intervalles de maintien en vie extrêmement courts peuvent incorrectement interrompre la connexion durant des périodes transitoires d'encombrement. Elles peuvent aussi causer un certain niveau de charge supplémentaire du réseau durant des périodes par ailleurs inactives.

Défaillance du collecteur se réfère à la défaillance ou au redémarrage du processus de collecte ou du collecteur lui-même. Une défaillance de collecteur est détectée à l'appareil IPFIX par la rupture de la session de protocole de transport en mode connexion ; selon le protocole de transport, les mécanismes de temporisation de connexion diffèrent. En détectant une fin de temporisation de maintien en vie dans un scénario à un seul collecteur, l'appareil IPFIX devrait cesser d'envoyer des enregistrements de flux au collecteur et essayer de rétablir la connexion de transport. Si la reprise sur défaillance du processus de collecte est prise en charge par le processus d'exportation, des sessions de sauvegarde peuvent être ouvertes à l'avance, et les informations de contrôle envoyées au processus de collecte de secours.

Il pourrait y avoit un ou plusieurs collecteurs secondaires avec des priorités allouées à chacun. La défaillance du collecteur principal est détectée à l'appareil IPFIX. En détectant la perte de connexité, l'appareil IPFIX ouvre un flux de données avec le collecteur secondaire de la plus haute priorité suivante. Si ce collecteur secondaire n'a pas été ouvert à l'avance, les informations de contrôle et le flux de donénes doivent toutes deux lui être envoyées. Ce collecteur pourrait alors devenir le principal, ou le processus d'exportation pourrait essayer de rétablir la session originale.

8.3 Redondance du collecteur

Configurer des collecteurs redondants est une solution de remplacement de la configuration de collecteurs de secours. Dans ce modèle, tous les collecteurs reçoivent simultanément les informations de contrôle et les flux de données. Plusieurs paires de{informations de contrôle, flux de données} pourraient être envoyées, chacune à un collecteur différent, provenant du même appareil IPFIX. Comme le protocole IPFIX exige un transport évitant l'encombrement, réaliser la redondance en utilisant la diffusion groupée n'est pas une option.

9. Collecte des flux IPFIX dans des situations particulières

Un appareil IPFIX peut générer, recevoir, et/ou altérer deux types particuliers de trafic, qui sont .

Trafic de tunnel : l'appareil IPFIX pourrait être le point d'entrée, un point médian, ou le point d'extrémité d'un tunnel. Dans ce cas, l'appareil IPFIX pourrait traiter du trafic d'encapsulation d'acheminement générique (GRE, *Generic Routing Encapsulation*) [RFC2784], IP dans IP [RFC1853], ou du protocole de tunnelage de couche 2, version 3 [RFC3931].

Trafic de VPN : l'appareil IPFIX pourrait être un appareil côté fournisseur qui reçoit du trafic provenant de sites de consommateurs appartenant à des réseaux privés virtuels différents.

De même, IPFIX pourrait être mis en œuvre sur des appareils qui effectuent un ou plusieurs des services particuliers suivants :
- o Paquets explicitement éliminés. Par exemple, un appareil qui fournit un service de pare-feu élimine des paquets sur la base d'une politique administrative.
- o Altérer la valeur des champs utilisés comme des clés de flux IPFIX intéressantes. Par exemple, un appareil qui fournit un service de NAT peut changer les adresses de source et/ou destination IP.

Dans des cas comme ceux ci-dessus, il devrait y avoir des lignes directrices claires sur :
- o Comment et quand classer les paquets comme des flux dans l'appareil IPFIX.
- o Si plusieurs encapsulations sont utilisées pour définir les flux, comment porter les mêmes champs (par exemple, adresse IP) dans les différentes couches.
- o Comment différencier les flux sur la base de domaines privés différents. Par exemple, des adresses IP qui se chevauchent dans des VPN de couche 3.
- o Quelles informations supplémentaires doivent être exportées afin que le collecteur puisse faire une interprétation claire des enregistrements de flux reçus.

10. Considérations sur la sécurité

Les informations de flux peuvent être utilisées pour divers objets, comme la comptabilité fondée sur l'usage, le profilage du trafic, l'ingénierie du trafic, et la détection d'intrusion. Les exigences de sécurité peuvent différer significativement pour de telles applications. Pour être capable de satisfaire les besoins de sécurité des divers utilisateurs IPFIX, un système IPFIX doit fournir différents niveaux de protection de la sécurité.

10.1 Sécurité des données

Les données IPFIX comprennent les informations de contrôle et les flux de données générés par l'appareil IPFIX.

Les données IPFIX peuvent exister dans l'appareil IPFIX et dans le collecteur. De plus, les données sont aussi transférées dans le réseau de l'appareil IPFIX au collecteur quand elles sont exportées. Pour assurer la sécurité, les données devraient être protégées contre les attaques courantes du réseau.

La protection des données IPFIX au sein du système d'extrémité (appareil IPFIX et collecteur) sort du domaine d'application du présent document. On suppose que l'opérateur du système d'extrémité va fournir une sécurité adéquate pour les données IPFIX.

L'architecture IPFIX doit permettre différents niveaux de protection aux données IPFIX dans le réseau. Partout où des fonctions de sécurité sont requises, il est recommandé que les utilisateurs s'appuient sur les couches inférieures en utilisant TLS ou DTLS (sécurité de la couche de transport de datagrammes) si elles peuvent réussir à satisfaire les exigences de

sécurité de la protection des données IPFIX.

Pour protéger les données dans le réseéau, trois niveaux de granularité devraient être pris en charge ; ils sont décrits dans les paragraphes qui suivent.

10.1.1 Sécurité fondée sur l'hôte

La sécurité peut n'être pas nécessaire quand le transport entre l'appareil IPFIX et le collecteur est perçue comme sûre. Cette option permet au protocole de fonctionner très efficacement sans frais généraux supplémentaires, et un système IPFIX doit la prendre en charge.

10.1.2 Authentification seule

La protection par l'authentification seule fournit aux utilisateurs IPFIX l'assurance de l'intégrité et de l'authenticité des données. Les données échangées entre l'appareil IPFIX et le collecteur sont protégées par une signature d'authentification. Toute modification des données IPFIX va être détectée par le receveur, résultant en l'élimination des données reçues. Cependant, l'option d'authentification seule n'offre pas la confidentialité des données.

L'utilisateur IPFIX ne devrait pas utiliser l'authentification seule quand des informations sensibles ou confidentielles sont échangées. Une solution IPFIX devrait prendre en charge cette option. L'option d'authentification seule devrait fournir la protection contre les attaques en répétition. Des moyens pour réaliser ce niveau de sécurité sont :

- L'encapsulation de la charge utile de sécurité (avec un algorithme de chiffrement nul).
- La sécurité de la couche transport (avec un algorithme de chiffrement nul).
- L'en-tête d'authentification IP.

10.1.3 Chiffrement

Le chiffrement des données fournit la meilleure protection pour les données IPFIX. Les données IPFIX sont chiffrées chez l'envoyeur, et seul le receveur prévu peut déchiffrer et avoir accès aux données. Cette option doit être utilisée quand le transport entre l'appareil IPFIX et le collecteur n'est pas sûr, et que les données IPFIX ont besoin d'être protégées. Il est recommandé que les fonctions de sécurité de la couche de transport sous-jacente soient utilisées à cette fin. Des moyens pour réaliser ce niveau de sécurité sont :

- l'encapsulation de charge utile de sécurité,
- le protocole de sécurité de la couche Transport.

L'option de chiffrement des données ajoute des frais généraux au transfert des données IPFIX. Elle peut limiter le taux auquel un exportateur peut rapporter ses enregistrements de flux au collecteur, du fait de l'exigence de ressource pour faire le chiffrement.

10.2 Authentification de point d'extrémité IPFIX

Il est important de s'assurer que l'appareil IPFIX parle au "bon" collecteur plutôt qu'à un collecteur déguisé. La même logique tient aussi du point de vue du collecteur, c'est-à-dire, il peut vouloir s'assurer qu'il collecte les enregistrements de flux provenant du "bon" appareil IPFIX. Un système IPFIX devrait permettre la capacité d'authentification des points d'extrémité afin qu'une authentification univoque ou mutuelle puisse être effectuée entre l'appareil IPFIX et le collecteur.

L'architecture IPFIX devrait utiliser tous les protocoles de protection du transport existants, comme TLS, pour satisfaire l'exigence d'authentification.

10.3 Surcharge de IPFIX

Un appareil IPFIX pourrait devenir surchargé dans diverses conditions. Cela peut être parce que les ressources internes utilisées pour la génération et/ou l'exportation de flux sont épuisées. Une telle surcharge peut causer la perte des données provenant du processus d'exportation, soit par manque de bande passante pour l'exportation (éventuellement causée par un nombre inhabituellement élevé de flux observés) soit par l'encombrement du réseau sur le chemin de l'exportateur au collecteur.

Les collecteurs IPFIX devraient être capables de détecter la perte des enregistrements de flux exportés, et devraient au

moins enregistrer le nombre d'enregistrements de flux perdus.

10.3.1 Prévention des attaques de déni de service (DoS)

Comme un des usages potentiels de IPFIX est la détection d'intrusion, il est important que l'architecture IPFIX prenne en charge une forme de résistance au DoS.

10.3.1.1 Réseau attaqué

Le réseau lui-même peut être attaqué, résultant en un nombre de messages IPFIX qui le submergent. Un système IPFIX devrait essayer de capturer autant d'informations que possible. Cependant, quand un grand nombre de messages IPFIX sont générés sur une courte période, le système IPFIX peut devenir surchargé.

10.3.1.2 Attaques génériques de DoS sur l'appareil et le collecteur IPFIX

L'appareil et le collecteur IPFIX peuvent être soumis à des attaques génériques de DoS, comme tout système sur un réseau ouvert. Ces types d'attaques ne sont pas spécifiques de IPFIX. Empêcher et répondre à ce type d'attaques sort du domaine d'application du présent document.

10.3.1.3 Attaques de DoS spécifiques de IPFIX

Il y a des attaques spécifiques sur la portion IPFIX de l'appareil ou collecteur IPFIX :

- L'attaquant pourrait submerger le collecteur avec des paquets d'exportation IPFIX falsifiés. Une façon de résoudre ce problème est de synchroniser périodiquement les numéros de séquence des enregistrements de flux entre les processus d'exportation et de collecte.

- L'attaquant pourrait fournir de faux rapports au collecteur en envoyant des paquets falsifiés.

Les problèmes mentionnés ci-dessus peuvent être résolus dans une large mesure si les paquets de contrôle sont chiffrés des deux côtés, fournissant ainsi plus d'informations que le collecteur pourrait utiliser pour identifier et ignorer les paquets de données falsifiés.

11. Considérations relatives à l'IANA

L'architecture IPFIX, telle qu'établie dans le présent document, a deux ensembles de numéros alloués, comme précisé dans les paragraphes qui suivent.

11.1 Numéros utilisés dans le protocole

Les messages IPFIX, comme décrit dans la [RFC5101], utilisent deux champs avec des valeurs allouées. Ce sont le numéro de version IPFIX, qui indique quelle version du protocole IPFIX a été utilisée pour exporter un message IPFIX, et l'identifiant d'ensemble IPFIX, qui indique le type de chaque ensemble d'informations au sein d'un message IPFIX.

Les valeurs pour le numéro de version IPFIX et l'identifiant d'ensemble IPFIX, avec les considérations sur leur allocation, sont définies dans la [RFC5101].

11.2 Numéros utilisés dans le modèle d'information

Les champs du protocole IPFIX portent des informations sur la mesure du trafic. Elles sont modélisée comme des éléments du modèle d'information IPFIX de la [RFC5102]. Chaque élément d'information décrit un champ qui peut apparaître dans un message IPFIX. Au sein d'un message IPFIX, le type de champ est indiqué par son Type de champ.

Les valeurs pour les identifiants d'élément d'information IPFIX, ainsi que les considérations sur leur allocation, sont définies dans la [RFC5102].

12. Remerciements

Les éditeurs de ce document souhaitent remercier toutes les personnes qui ont contribué aux discussions sur ce document sur la liste de diffusion, et les équipes de conception, pour leurs nombreux commentaires précieux. En particulier, les personnes suivantes ont fait des contributions significatives : Tanja Zseby, Paul Calato, Dave Plonka, Jeffrey Meyer, K.C. Norseth, Vamsi Valluri, Cliff Wang, Ram Gopal, Jc Martin, Carter Bullard, Reinaldo Penno, Simon Leinen, Kevin Zhang, Paul Aitken, Brian Trammell.

Des remerciement particuliers à Dave Plonka pour ses nombreuses relectures.

13. Références

13.1 Références normatives

[RFC3917] J. Quittek, T. Zseby, B. Claise, S. Zander, "Exigences pour l'exportation d'informations de flux IP (IPFIX)", octobre 2004. *(Information)*

[RFC5101] B. Claise, éd., "Spécification du protocole d'exportation d'informations de flux IP (IPFIX) pour l'échange d'informations de flux de trafic IP", janvier 2008. *(P.S.) (Obsolète, voir* RFC7011, STD77)

[RFC5102] J. Quittek et autres, "Modèle d'informations pour l'exportation d'informations de flux IP", janvier 2008. *(P.S.) (Remplacée par* RFC7012)

[RFC5472] T. Zseby et autres, "Applicabilité de l'exportation d'information de flux IP (IPFIX)", mars 2009. *(Info.)*

13.2 Références pour information

[RFC1853] W. Simpson, "Tunnel IP dans IP", octobre 1995. *(Information)*

[RFC2784] D. Farinacci, T. Li, S. Hanks, D. Meyer et P. Traina, "Encapsulation d'acheminement générique (GRE)", DOI 10.17487/RFC2784, mars 2000.

[RFC3550] H. Schulzrinne, S. Casner, R. Frederick et V. Jacobson, "RTP : un protocole de transport pour les applications en temps réel", STD 64, juillet 2003. *(MàJ par* RFC7164, RFC7160, RFC8083, RFC8108, RFC8860)

[RFC3931] J. Lau et autres, "Protocole de tunnelage de couche deux - version 3 (L2TPv3)", DOI 10.17487/RFC3931, mars 2005. *(P.S.)*

[RFC3955] S. Leinen, "Évaluation des protocoles candidats pour l'exportation d'informations de flux IP (IPFIX)", octobre 2004. *(Information)*

Adresse des auteurs

Ganesh Sadasivan
Rohati Systems
1192 Borregas Ave.
Sunnyvale, CA 94089
USA
mél : gsadasiv@rohati.com

Nevil Brownlee
CAIDA | The University of Auckland
Private Bag 92019
Auckland 1142
New Zealand
téléphone : +64 9 373 7599 x88941
mél : n.brownlee@auckland.ac.nz

Benoit Claise
Cisco Systems, Inc.

Juergen Quittek
NEC Laboratories Europe, NEC Europe Ltd.

De Kleetlaan 6a b1
1831 Diegem
Belgium
téléphone : +32 2 704 5622
mél : bclaise@cisco.com

Kurfuersten-Anlage 36
Heidelberg 69115
Germany
téléphone : +49 6221 4342-115
mél : quittek@nw.neclab.eu