Groupe de travail Réseau
Request for Comments : 5103
Catégorie : Sur la voie de la normalisation
Traduction Claude Brière de L'Isle

B. Trammell, CERT/NetSA
E. Boschi, Hitachi Europe
janvier 2008

Exportation de flux bidirectionnel en utilisant l'exportation d'informations de flux IP (IPFIX)

Résumé
Le présent document décrit une méthode efficace pour exporter des informations de flux bidirectionnels (biflux) en utilisant le protocole d'exportation de flux IP (IPFIX, *IP Flow Information Export*) représentant chaque biflux à l'aide d'un seul enregistrement de flux.

Table ds Matières

1. Introduction

De nombreuses tâches d'analyse de flux bénéficient de l'association des flux vers l'amont et vers l'aval avec une communication bidirectionnelle, par exemple, séparant les demandes TCP qui ont eu une réponse et celles qui n'en ont pas eu, calculant les temps d'aller-retour, etc. Les processus de mesure qui ne font pas partie d'une infrastructure d'acheminement asymétrique, en particulier celles déployée à un seul point à travers lequel s'écoule le trafic bidirectionnel, sont bien positionnés pour observer les flux bidirectionnels (biflux). Dans ces topologies, les exigences totales de ressources pour l'assemblage de biflux sont souvent inférieures si les biflux sont assemblés à l'interface de mesure plutôt qu'au collecteur. Le protocole IPFIX exige seulement des extensions au modèle d'informations qui soient complètes comme solution pour l'exportation des données de biflux.

À cette fin, on propose dans le présent document une méthode d'exportation de biflux qui utilise un seul enregistrement de flux par biflux. On explore la sémantique des données de flux bidirectionnel dans la Section 4, "Sémantique de biflux" ; on examine les diverses possibilités pour déterminer la direction des biflux dans la Section 5, "Allocation de direction" ; puis on définit la méthode d'exportation de biflux dans la Section 6, "Représentation d'enregistrement".

Cette méthode d'exportation exige des éléments d'information supplémentaires pour représenter les valeurs des données pour la direction inverse de chaque biflux, et un seul élément d'information supplémentaire pour représenter les informations d'allocation de direction, comme décrit aux paragraphes 6.1 à 6.3. Le choix de cette méthode est motivé par une exploration des autres méthodes possibles d'exportation de biflux utilisant IPFIX ; cependant, ces méthodes ont des inconvénients importants, comme exposé à la Section 3, "Raisons et historique".

1.1 Vue d'ensemble des documents IPFIX

La "Spécification du protocole IPFIX pour l'échange d'informations de flux de trafic IP" [RFC5101] (informellement, le document de protocole IPFIX) et ses documents associés définit le protocole IPFIX, qui donne aux ingénieurs et administrateurs de réseau l'accès aux informations de flux de trafic IP.

"Architecture pour l'exportation d'informations de flux IP" [RFC5470] (le document d'architecture IPFIX) définit l'architecture pour l'exportation des informations de flux IP mesurées à partir d'un processus d'exportation IPFIX vers un processus de collecte IPFIX, et la terminologie de base utilisée pour décrire les éléments de cette architecture, selon les exigences définies dans "Exigences pour l'exportation des informations de flux IP" [RFC3917]. Le document de protocole IPFIX [RFC5101] couvre alors les détails de la méthode de transport des enregistrements et gabarits de données IPFIX via un protocole de transport conscient des problèmes d'encombrement depuis un processus d'exportation IPFIX jusqu'à un processus de collecte IPFIX.

Le "Modèle d'information pour l'exportation des informations de flux IP" [RFC5102] (informellement, appelé le document de modèle d'informations IPFIX) décrit les éléments d'information utilisés par IPFIX, incluant les détails sur la dénomination des éléments d'information, leur numérotation, et le codage du type de données. Finalement, "Applicabilité de IPFIX" [RFC5472] décrit les diverses applications du protocole IPFIX et leur utilisation des informations exportées via IPFIX, et traite de l'architecture IPFIX en relation avec les autres architectures et cadres de mesure IPFIX.

Le présent document fait référence aux documents de protocole et d'architecture pour la terminologie, utilise le protocole IPFIX pour définir une méthode d'export de flux bidirectionnel, et propose des ajouts au modèle d'information défini dans le document de modèle d'information IPFIX.

2. Terminologie

Les termes utilisés dans ce document qui sont définis dans la Section Terminologie du document de protocole IPFIX [RFC5101] sont à interpréter comme ils y sont définis. Les termes supplémentaires suivants sont définis dans les termes de la terminologie du document de protocole IPFIX.

Champ Clé de direction : c'est un seul champ dans une clé de flux, comme défini dans le document de protocole IPFIX [RFC5101] qui est spécifiquement associé à un seul point d'extrémité du flux. Des exemples de champs de clé de direction sont sourceIPv4Address et destinationTransportPort.

Champ Clé non directionnelle : c'est un seul champ dans une clé de flux, comme défini dans le document de protocole IPFIX [RFC5101] qui n'est pas spécifiquement associé à l'un ou l'autre point d'extrémité du flux. Un exemple de champ Clé non directionnelle est protocolIdentifier.

Uniflux (flux unidirectionnel) : un uniflux est un flux comme défini dans le document de protocole IPFIX [RFC5101], restreint de telle façon que le flux soit composé seulement de paquets envoyés d'un seul point d'extrémité à un seul autre point d'extrémité.

Biflux (flux bidirectionnel) : un biflux est un llux comme défini dans le document de protocole IPFIX [RFC5101], composé de paquets envoyés dans les deux directions entre deux points d'extrémité. Un biflux est composé de deux uniflux tels que :

1. la valeur de chaque champ Clé non directionnelle de chaque uniflux est identique à sa contrepartie dans l'autre, et
2. la valeur de chaque champ Clé de direction de chaque uniflux est identique à sa contrepartie dans la direction inverse chez l'autre.

Un biflux contient deux champs non de clé pour chaque valeur qu'il représente associés à une seule direction ou point d'extrémité : un pour la direction vers l'avant et un pour la direction inverse, comme défini ci-dessous.

source de biflux : la source de biflux est le point d'extrémité identifié par le champ Clé de direction de source dans le biflux.

destination de biflux : c'est le point d'extrémité identifié par les champs Clé de direction de destination dans le biflux.

direction vers l'avant (d'un biflux) : direction d'un biflux composé de paquets envoyés par la source de biflux. Les valeurs associées à la direction vers l'avant d'un biflux sont représentées en utilisant les éléments d'information normaux. En d'autres termes, un uniflux peut être défini comme un biflux ayant seulement une direction vers l'avant.

direction inverse (d'un biflux) : direction d'un biflux composé de paquets envoyés de la destination de biflux. Les valeurs associées à la direction inverse d'un biflux sont représentées en utiliant les éléments d'information inverses, comme défini ci-dessous.

élément d'information inverse : un élément d'information défini comme correspondant à un élément d'information normal (ou vers l'avant) mais associé à la direction inverse d'un biflux.

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

3. Raisons et historique

En choisissant la méthode d'exportation d'un seul enregistrement de biflux décrite dans le présent document comme recommandation pour l'exportation de flux bidirectionnel à l'aide de IPFIX, on a considéré plusieurs autres méthodes possibles.

La première et la plus évidente serait de simplement exporter les biflux comme deux uniflux adjacents dans le flux d'enregistrements ; un processus collecteur pourrait alors les réassembler avec des exigences d'état minimales. Cependant, cela a l'inconvénient que s'est simplement un arrangement informel sur lequel le processus collecteur ne peut pas s'appuyer, et ce n'est pas efficace en bande passante, dupliquant l'exportation des données de clé de flux dans chaque enregistrement d'uniflux.

On a ensuite considéré la méthode proposée dans les rapports de redondance réduite dans IPFIX et d'échantillonnage de paquets (PSAMP, *Packet Sampling*) [RFC5473] pour réduire cette inefficacité en bande passante. Cela lierait aussi formellement les deux uniflux en une seule construction, en exportant la clé de flux comme une propriété commune puis en exportant les informations de chaque direction comme des propriétés spécifiques. Cependant, ce serait aux dépens de frais généraux supplémentaires pour transmettre l'identifiant de propriétés communes, et des exigences de gestion d'état supplémentaires aux processus collecteur et exportateur.

Une proposition avait été faite sur la liste de diffusion IPFIX d'utiliser la caractéristique d'élément d'information multiple du protocole pour exporter les compteurs vers l'avant et inverse en utilisant des éléments d'information identiques dans le même enregistrement de flux. Dans cette approche, la première instance d'un compteur aurait représenté la direction vers l'avant, et la seconde instance du même compteur la direction inverse. Cela présente l'inconvénient d'entrer en conflit avec la sémantique présentement définie pour ces compteurs, et elle a été abandonnée pour cette raison.

4. Sémantique de biflux

Comme indiqué dans la section de terminologie, un biflux est simplement un flux qui représente des paquets qui s'écoulent dans les deux directions entre deux points d'extrémité sur un réseau. Il y a des raisons impérieuses de traiter les biflux comme une seule entité (par opposition à simplement des combinaisons ad-hoc d'uniflux) au sein de IPFIX. D'abord, comme la plupart des protocoles réseau de couche d'application sont par nature bidirectionnels, un modèle de données fondé sur le biflux reprèsente plus précisément le comportement du réseau, et permet une application plus aisée des flux de données pour répondre aux questions qui intéressent le comportement du réseau. Ensuite, l'exportation des données de biflux peut résulter en une efficacité accrue de l'exportation en éliminant la duplication des données de clé de flux dans un flux de messages IPFIX, et améliorer l'efficacité de la collecte en retirant lorsque possible le fardeau de la confrontation de biflux au processus collecteur.

Les biflux sont un peu plus compliqués sémantiquement que les uniflux. Quand on traite des uniflux, la sémantique des éléments d'information de source et destination est clairement définie par la sémantique des données d'en-tête de paquet sous-jacentes : les éléments d'information de source représentent les champs d'en-tête de source, et les éléments d'information de destination représentent les champs d'en-tête de destination. Quand on représente des biflux avec un seul enregistrement de données IPFIX, les définitions de source et destination doivent être choisies avec plus de soins.

Comme dans la section de terminologie ci-dessus, on définit la source d'un biflux comme étant identifiée par le ou les champs de clé de direction de source, et la destination du biflux comme étant identifiée par le ou les champs de clé de direction de destination. Noter que pour les éléments d'information enregistrés par l'IANA, ou ceux définis par le modèle d'information IPFIX [RFC5102], les champs de clé de direction associés à la source de biflux sont représentés par des éléments d'information dont les noms commencent par "source", et les champs de clé de direction associés aux biflux de destination sont représentés par des éléments d'information dont les noms commencent par "destination" ; il est recommandé que les éléments d'information spécifiques d'entreprise suivent aussi ces conventions.

Les méthodes pour allouer la source et la destination par les processus de mesure et exportateur sont décrites au paragraphe suivant.

Comme la source et la destination d'un biflux sont définies dans les termes de leurs clés de direction, les valeurs de biflux sont aussi partagées en directions vers l'avant et inverse. Comme dans la section de terminologie ci-dessus, la direction vers l'avant d'un biflux est composée des paquets envoyés par la source de biflux, et la direction inverse d'un biflux est composée des paquets envoyés par la destination. En d'autres termes, les deux directions d'un biflux peuvent être vues en gros comme deux uniflux qui ont été confrontés pour composer le biflux. Un enregistrement de biflux, contient alors une fois chaque enregistrement de clé de flux, et les deux éléments d'information vers l'avant et inverse pour chaque champ non de clé. Voir à la Figure 1 une illustration de la composition des biflux à partir des uniflux.

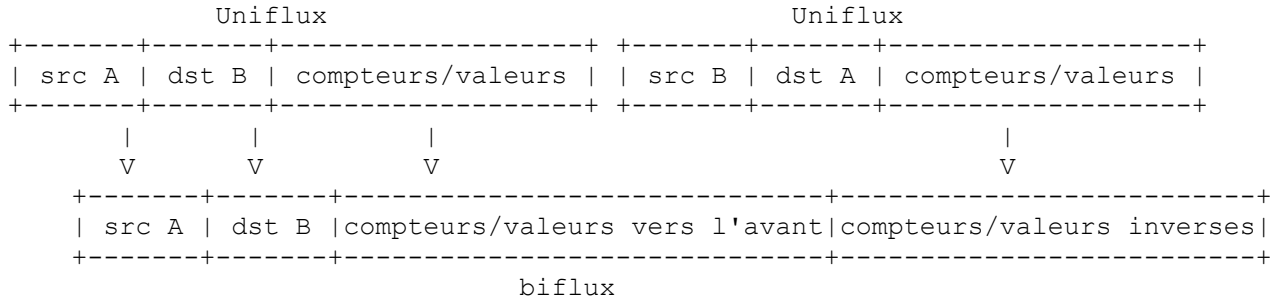


Figure 1 : diagramme conceptuel de flux bidirectionnel

Les valeurs de direction inverse sont représentées par les éléments d'information inverses. La représentation de ces éléments d'information inverses au sein des gabarits est détaillée à la Section 5. Un enregistrement de flux peut être considéré comme étant un enregistrement de biflux par le processus collecteur si il contient au moins un élément d'information inverse ET au moins un champ de clé de direction. Les enregistrements de flux qui contiennent des éléments d'information inverses mais pas de champs de clé de direction sont illégaux, NE DOIVENT PAS être envoyés par le processus d'exportation, et DEVRAIENT être éliminés par le processus collecteur. Le processus collecteur DEVRAIT enregistrer la réception de tels enregistrements de flux illégaux.

Quand il exporte des uniflux, le processus exportateur DEVRAIT utiliser un gabarit ne contenant pas d'élément d'information inverse. Noter qu'un gabarit dont les seuls éléments d'information inverses sont des compteurs PEUT être utilisé pour exporter des uniflux, comme des compteurs dont les valeurs de 0 sont sémantiquement équivalentes à pas de direction inverse. Cependant, cette approche n'est pas possible pour les éléments d'information inverses dont les valeurs de zéro ont une signification distincte (par exemple, tcpControlBits).

Noter qu'un biflux qui traverse un boîtier de médiation [RFC3234] peut exposer des propriétés de flux différentes sur chaque côté du boîtier de médiation à cause de changements à l'en-tête ou à la charge utile de paquet effectués par le boîtier de médiation lui-même. Donc, il DOIT être clair à un processus collecteur si les paquets ont été observés et mesurés avant ou après la modification. Le processus d'observation DEVRAIT être localisé sur un côté d'un boîtier de médiation, et le processus d'exportation DEVRAIT communiquer au processus collecteur les valeurs entrantes des propriétés du flux qui ont changé au sein du boîtier de médiation et les valeurs changées "de l'autre côté". Le modèle d'information IPFIX [RFC5102] fournit des éléments d'information avec le préfixe "post" à cette fin. La localisation du ou des points d'observation par rapport au boîtier de médiation peut être communiquée en utilisant des options avec le point d'observation comme portée et des éléments tels que lineCardID ou samplerID.

Pour plus d'informations sur les effets des boîtiers de médiation dans l'architecture IPFIX, voir la Section 7 des lignes directrices pour la mise en œuvre de IPFIX [RFC5153].

Selon la définition du domaine d'observation à la Section 2 du document de protocole IPFIX [RFC5101], des biflux peuvent être seulement composés de paquets observés dans le même domaine d'observation. Cela implique que le processus de mesure qui construit des biflux à partir d'uniflux doit s'assurer que les deux uniflux ont été observés dans le même domaine d'observation.

5. Allocation de direction

Du fait de la diversité des applications de mesure de flux et des restrictions sur le déploiement de processus de mesure, une seule méthode d'allocation des directions d'un biflux ne va pas s'appliquer dans tous les cas. Cette section décrit trois méthodes d'allocation de direction, et les recommande sur la base des positions de processus de mesure et des exigences d'application de mesure. Dans chacune des figures de cette section, la boîte "MP" représente le processus de mesure.

Comme le choix de la méthode dépend de la position du processus de mesure, il est suffisant de configurer la méthode d'allocation de direction au processus de collecte et/ou au processus d'exportation hors bande. Par exemple, un processus collecteur pourrait être configuré pour qu'un processus d'exportation spécifique identifié par exporterIPv4Address alloue une direction par initiateur ; ou qu'un processus collecteur et un processus d'exportation pourraient être simultanément configurés avec un périmètre spécifique d'allocation de direction. Cependant, pour un processus exportateur qui utilise plusieurs méthodes de choix de direction, ou pour des processus de collecte qui acceptent des données d'un processus exportateur qui utilise diverses méthodes, un élément d'information biflowDirection est fourni pour une représentation facultative des informations d'allocation de direction.

5.1 Direction par initiateur

Si l'application de mesure exige la détermination de l'initiateur et du répondeur d'une certaine communication, le processus de mesure DEVRAIT définir la source du biflux comme étant l'initiateur du biflux, lorsque possible. Cela peut être approximé en gros par un processus de mesure qui observe les paquets dans les deux directions en supposant simplement que le premier paquet vu dans un biflux donné est le paquet qui initie le biflux. Un processus de mesure peut améliorer cette méthode en utilisant la connaissance des protocoles de transport ou d'application (par exemple, des fanions TCP, des comptes de question/réponse au DNS) pour mieux approximer le paquet qui initie le flux.

Noter que l'allocation de la direction par l'initiateur est faite très facilement par un seul processus de mesure positionné sur une couche de liaison locale, comme dans la Figure 2, ou un seul processus de mesure observant les flux de paquets bidirectionnels à un point d'acheminement de périmètre symétrique, comme dans la Figure 3.

Noter aussi que de nombreux processus de mesure ont une temporisation "active", telle que tout flux d'une durée supérieure à la temporisation active se termine et que tous les autres paquets appartenant à ce flux soient comptés comme faisant partie d'un nouveau flux. Ce mécanisme peut causer des problèmes dans l'hypothèse où un premier paquet vu est du flux initiateur, si le "premier" paquet est un paquet au milieu d'un flux de longue durée.

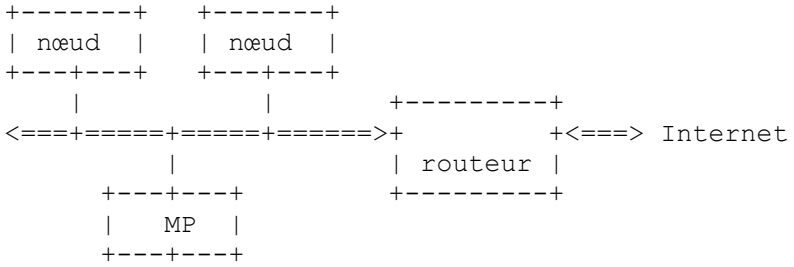


Figure 2 : Position d'un processus de mesure de liaison locale

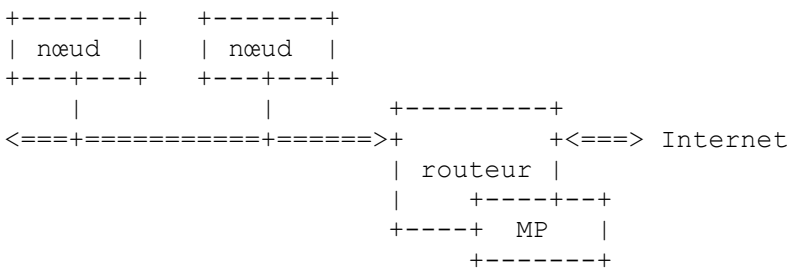


Figure 3 : Position d'un processus de mesure de point d'acheminement symétrique

5.2 Direction par périmètre

Si l'application de mesure est déployée à un périmètre de réseau, comme illustré à la Figure 4, de telle façon qu'il y ait un ensemble stable d'adresses qui peut être défini comme "à l'intérieur" de ce périmètre, et qu'il n'y a pas d'exigence d'application de mesure pour déterminer l'initiateur et le répondeur d'une certaine communication, alors le processus de mesure DEVRAIT allouer la source du biflux comme étant le point d'extrémité qui est en dehors du périmètre.

Aucune facilité n'est fournie pour exporter l'ensemble d'adresses qui définit l'intérieur d'un périmètre ; cet ensemble peut être déduit par le processus collecteur en observant l'ensemble d'adresses de source et de destination du biflux, ou être configuré hors bande.

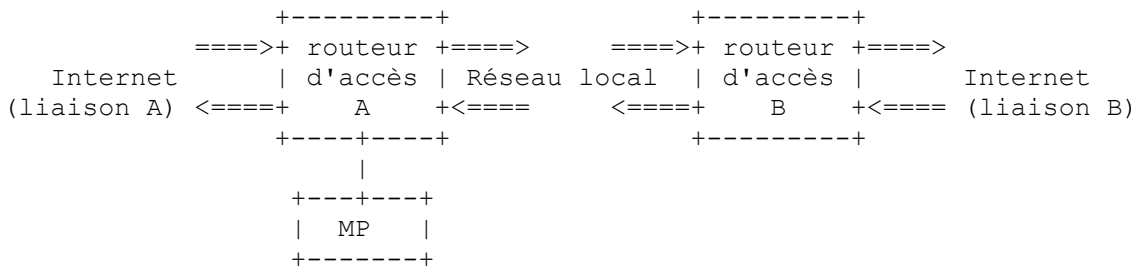


Figure 4 : Position de processus de mesure de périmètre

5.3 Direction arbitraire

Si l'application de mesure est déployée dans un cœur de réseau, de sorte qu'il n'y a pas d'ensemble stable d'adresses définissant un périmètre (par exemple, du fait de mises à jour BGP) comme dans la Figure 5, et pas d'exigence ou de capacité de déterminer l'initiateur ou le répondeur d'une certaine communication, alors le processus de mesure PEUT alllouer arbitrairement les points d'extrémité de source et de destination du biflux.

Dans ce cas, le processus de mesure DEVRAIT être cohérent dans son choix de direction. Une fois allouée, la direction DEVRAIT être conservée pour la durée de vie du biflux, même dans le cas de temporisation active d'un biflux de longue durée.

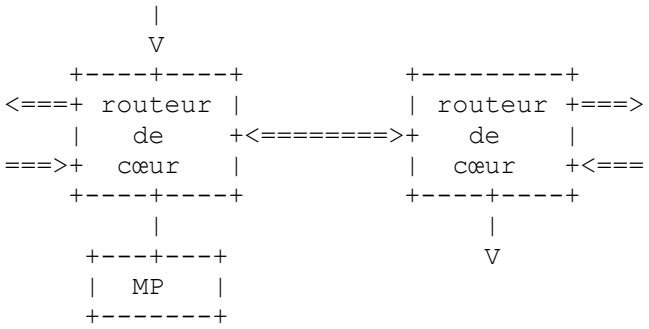


Figure 5 : Position de processus de mesure de transit/cœur

6. Représentation d'enregistrement

Comme noté ci-dessus, des biflux sont exportés en utilisant un seul enregistrement de flux, dont chacun contient les champs de clé de flux une fois, et les deux éléments d'information vers l'avant et les éléments d'information inverses pour chaque champ non de clé. Le modèle d'information IPFIX est étendu pour fournir un élément d'information inverse en contrepartie de chaque élément d'information vers l'avant présentement défini, comme requis par tout élément d'information qui peut être un champ non de clé dans un biflux.

6.1 Élément d'information inverse Numéro d'entreprise privée

Les éléments d'information inverses sont spécifiés comme une "dimension" séparée dans l'espace d'éléments d'information, en allouant le numéro d'entreprise privée (PEN, *Private Enterprise Number*) 29305 à ce document, et en définissant qu'un PEN signifie un "élément d'information inverse IPFIX" (le PEN inverse). Ce PEN inverse sert de "fanion Direction inverse" dans le gabarit ; chaque numéro d'élément d'information au sein de cet espace de PEN est alloué à la contrepartie inverse du numéro d'élément d'information public alloué par l'IANA correspondant. En d'autres termes, pour générer un élément d'information inverse dans un gabarit correspondant à un certain élément d'information vers l'avant, on établit simplement le bit entreprise et on définit l'élément d'information au sein de l'espace PEN inverse, comme dans la Figure 6.

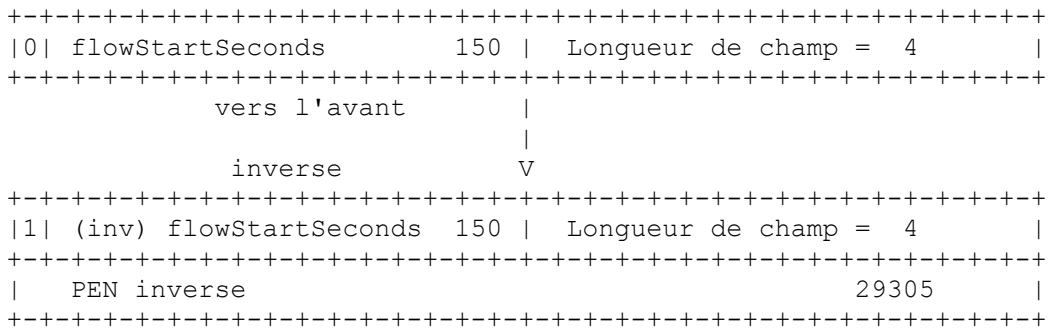


Figure 6 : Exemple de transpostion entre IE vers l'avant et inverse

Comme la dimension d'élément d'information inverse est traitée explicitement comme telle, de nouveaux éléments d'information peuvent être librement ajoutés à l'espace géré par l'IANA sans se soucier de savoir si un élément d'information inverse devrait aussi être ajouté. À côté de l'allocation initiale d'un numéro d'entreprise privée pour cela, il n'y a pas de frais généraux de maintenance supplémenaires pour prendre en charge les éléments d'information inverses dans le modèle d'information IPFIX.

Noter que certains éléments d'information dans le modèle d'information IPFIX [RFC5102] ne sont pas réversibles ; c'est-à-dire, ils n'ont pas de signification comme éléments d'information inverses. Un processus d'exportation NE DOIT PAS exporter un gabarit contenant la contrepartie inverse d'un élément d'information non réversible. Un processus collecteur qui reçoit la contrepartie inverse d'un élément d'information non réversible PEUT éliminer cet élément d'information de l'enregistrement de flux. Les éléments d'information non réversibles représentent les propriétés de l'enregistrement de biflux comme un tout, ou sont destinés à l'usage interne du protocole IPFIX lui-même. Donc, par définition, ils ne peuvent pas être associés à une seule direction ou point d'extrémité du flux.

Les éléments d'information spécifiques suivants ne sont pas reversibles :

1. Identifiants définis au paragraphe 5.1 de la [RFC5102] qui ne peuvent pas être associés à une seule direction de collection d'uniflux : flowId (5.1.7), templateId (5.1.8), observationDomainId (5.1.9), et commonPropertiesId (5.1.11).
2. Éléments de configuration de processus définis au paragraphe 5.2 de la [RFC5102].
3. Éléments de statistiques de processus définis au paragraphe 5.3 de la [RFC5102].
4. paddingOctets défini au paragraphe 5.12.1 de la [RFC5102].
5. biflowDirection (défini au paragraphe 6.3 du présent document).

Tout futur ajout au registre des éléments d'information de l'IANA qui satisfait aux critères définis ci-dessus DEVRAIT aussi être considéré comme étant non réversible par le processus collecteur.

Noter que les éléments d'information couramment utilisés comme clé de flux (par exemple, les champs d'en-tête définis au paragraphes 5.4 et 5.5 du modèle d'information) sont réversibles, car ils peuvent être utilisés comme des champs de valeur dans certains contextes, comme lorsque ils associent des messages d'erreur ICMP aux flux qui les ont causés.

6.2 Élément d'information inverse spécifiques de l'entreprise

Noter que le PEN inverse défini ci-dessus est seulement disponible pour allouer les contreparties inverses des éléments d'information IPFIX enregistrés par l'IANA. Aucune facilité n'est fournie pour allouer les contreparties inverses des éléments d'information spécifiques d'entreprise.

L'allocation des éléments d'information spécifiques d'entreprise pour IPFIX est laissée à la discrétion de l'organisation qui les alloue. Noter que les éléments d'information spécifiques d'entreprise sont conçus pour l'usage interne des entreprises privées, l'absence de lignes directrices standard sur les politiques d'allocation d'élément d'information ne pose aucun problème d'interopérabilité. Cependant, si le propre registre des éléments d'information d'une entreprise privée anticipe l'allocation d'éléments d'information réversibles, et si l'utilisation de cette spécification pour l'exportation de données de biflux, ce registre PEUT réserver un des quinze bits disponibles dans l'identifiant d'élément d'information pour signifier la direction inverse. Par exemple, si le bit de poids fort est choisi, cela va réserver les identifiants d'élément d'information 0x4000 à 0x7FFF pour la direction inverse des identifiants d'élément d'information 0x0000 à 0x3FFF.

6.3 Élément d'information biflowDirection

Description : une description de la méthode d'allocation de direction utilisée pour allouer la source et la destination de biflux. Cet élément d'information PEUT être présent dans un enregistrement de flux, ou appliqué à tous les flux exportés d'un processus d'exportation ou d'un domaine d'observation utilisant les options IPFIX. Si cet élément d'information n'est pas présent dans un enregistrement de flux ou associé à un biflux via une portée, on supposera que la configuration de la méthode d'allocation de direction est faite hors bande. Noter que quand on utilise les options IPFIX pour appliquer cet élément d'information à tous les flux au sein d'un domaine d'observation ou à partir d'un processus d'exportation, l'option DEVRAIT être envoyé de façon fiable. Si un transport fiable n'est pas disponible (c'est-à-dire, quand on utilise UDP) cet élément d'information DEVRAIT apparaître dans chaque enregistrement de flux. Ce champ peut prendre les valeurs suivantes :

Valeur	Nom	Description
0x00	arbitraire	La direction allouée est arbitraire.
0x01	initiateur	La source de biflux est le flux initiateur, comme déterminé par le mieux que peut faire le processus de mesure pour détecter l'initiateur.
0x02	reverseInitiator	La destination du biflux est le flux initiateur, comme déterminé par le mieux que peut faire le processus de mesure pour détecter l'initiateur. Cette valeur est fournie pour l'agrément du processus exportateur pour réviser l'estimation d'un initiateur sans re-coder l'enregistrement de biflux.
0x03	périmètre	La source de biflux est le point d'extrémité en-dehors d'un périmètre défini. La définition du périmètre est implicite dans l'ensemble des adresses de source de biflux et de destination de biflux exporté dans les enregistrements de biflux.

Type de données abstrait : unsigned8

Sémantique du type de données : identifiant

ElementId : 239

Statut : courant

7. Considérations relatives à l'IANA

Le présent document spécifie la création d'une nouvelle dimension dans l'espace d'éléments d'information défini par le modèle d'information IPFIX [RFC5102]. Cette nouvelle dimension est définie par l'allocation d'un nouveau numéro d'entreprise privée (PEN, *Private Enterprise Number*). L'Autorité d'allocation des numéros de l'Internet (IANA, *Internet Assigned Numbers Authority*) a alloué le numéro d'entreprise privée 29305 au présent document comme "élément d'information inverse IPFIX Entreprise privée", avec les auteurs du présent document comme point de contact.

Le présent document spécifie la création d'un nouvel élément d'information IPFIX, "biflowDirection", comme défini au paragraphe 6.3. L'IANA lui a alloué le numéro d'élément d'information 239 dans le registre des éléments d'information IPFIX. Les valeurs définies pour cet élément d'information sont statiques, et n'ont donc pas besoin d'être tenues dans un sous registre par l'IANA.

8 Considérations sur la sécurité

Les mêmes considérations de sécurités que pour le protocole IPFIX [RFC5101] s'appliquent.

9. Remerciements

Nous tenons à remercier Lutz Mark, Juergen Quittek, Andrew Johnson, Paul Aitken, Benoit Claise, et Carsten Schmoll de leurs contributions et commentaires. Des remerciements partis à Michelle Cotton pour son assistance à la navigation dans les processus de l'IANA pour l'allocation de numéro d'entreprise, et pour la relecture du document par l'IANA avant sa publication.

10. Références

10.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[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)

10.2 Références pour information

[RFC3234] B. Carpenter, S. Brim, "Boîtiers de médiation : taxonomie et problèmes", février 2002. *(Information)*

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

[RFC5153] E. Boschi et autres, "Lignes directrices pour la mise en œuvre de IPFIX", avril 2008. *(Information)*

[RFC5470] G. Sadasivan et autres, "Architecture pour l'exportation d'informations de flux IP", mars 2009. *(Information)*

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

[RFC5473] E. Boschi et autres, "Réduction de redondance dans les rapports d'exportation d'informations de flux IP (IPFIX) et d'échantillonnage de paquet (PSAMP)", mars 2009. *(Information)*

Appendice A. Exemples

L'exemple suivant décrit un enregistrement de biflux comme spécifié à la Section 6 ci-dessus. Le PEN inverse est alloué pour différencier les éléments d'information vers l'avant des inverses.

Les informations exportées dans ce cas sont :

- L'heure de début du flux : flowStartSeconds dans le modèle d'information IPFIX [RFC5102], de 4 octets.
- L'heure de début du flux inverse : flowStartSeconds dans le modèle d'information IPFIX [RFC5102], de 4 octets, et le bit Entreprise réglé à 1. Le PEN suivant est le PEN inverse.
- L'adresse IPv4 de source : sourceIPv4Address dans le modèle d'information IPFIX [RFC5102], de 4 octets.
- L'adresse IPv4 de destination : destinationIPv4Address dans le modèle d'information IPFIX [RFC5102], de 4 octets.
- L'accès de source : sourceTransportPort dans le modèle d'information IPFIX [RFC5102], de 2 octets.
- L'accès de destination : destinationTransportPort dans le modèle d'information IPFIX [RFC5102], de 2 octets.
- L'identifiant de protocole : protocolIdentifier dans le modèle d'information IPFIX [RFC5102], de 1 octet.
- Le nombre d'octets du flux : octetTotalCount dans le modèle d'information IPFIX [RFC5102], de 4 octets.

- o Le nombre inverse d'octets du flux : octetTotalCount dans le modèle d'information IPFIX [RFC5102], de 4 octets, et le bit Entreprise réglé à 1. Le PEN suivant est le PEN inverse.
- o Le nombre de paquets du flux : packetTotalCount dans le modèle d'information IPFIX [RFC5102], de 4 octets.
- o Le nombre inverse de paquets du flux : packetTotalCount dans le modèle d'information IPFIX [RFC5102], de 4 octets, et le bit Entreprise réglé à 1. Le PEN suivant est le PEN inverse.

Le gabarit d'ensemble résultant ressemblerait au diagramme ci-dessous :

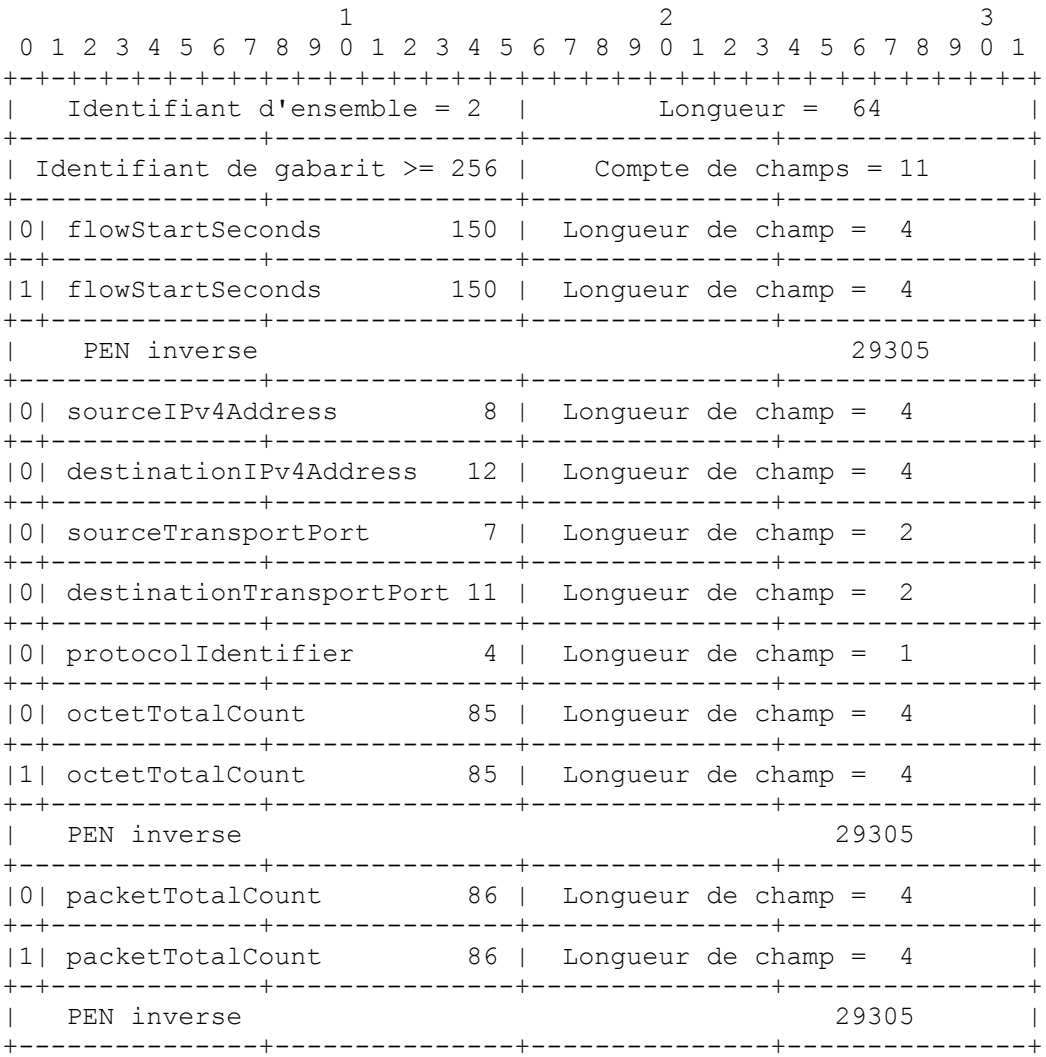
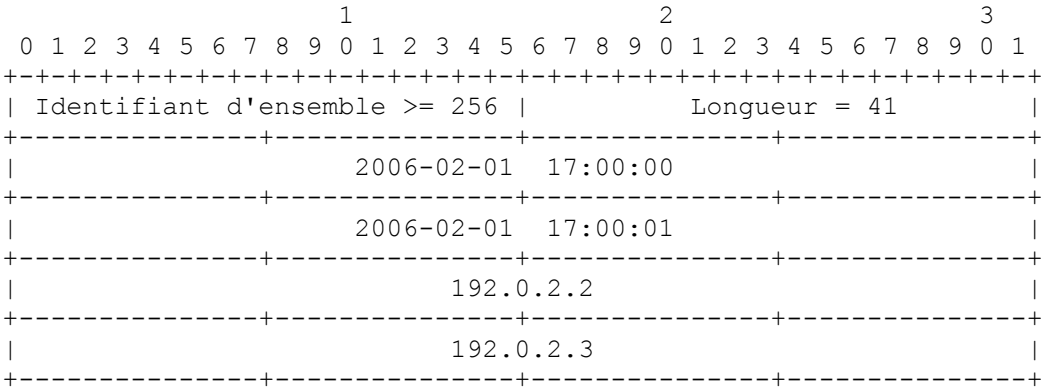


Figure 7 : Gabarit d'ensemble d'un seul enregistrement de biflux

L'exemple suivant d'ensemble de données représente une transaction HTTP typique. Son format est défini par l'exemple de gabarit ci-dessus.



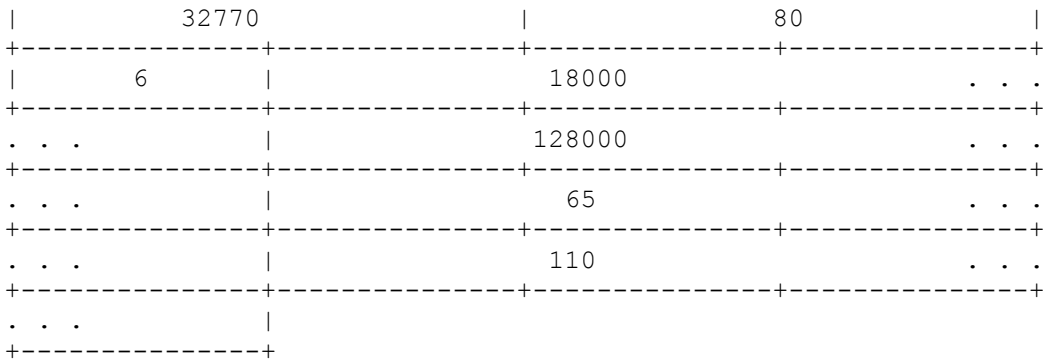


Figure 8 : Ensemble de données d'un seul enregistrement de biflux

L'exemple suivant montre l'utilisation de l'élément d'information biflowDirection, comme spécifié au paragraphe 6.2, en utilisant le mécanisme d'options IPFIX pour spécifier que le choix de direction de périmètre est effectué pour un certain domaine d'observation.

Les informations exportées dans ce cas sont :
- o domaine d'observation : observationDomainId dans le modèle d'information IPFIX [RFC5102], de 4 octets.
- o méthode d'allocation de direction : biflowDirection comme défini au paragraphe 6.2, de 1 octet.

Le gabarit résultant d'ensemble d'options ressemblerait au diagramme ci-dessous :

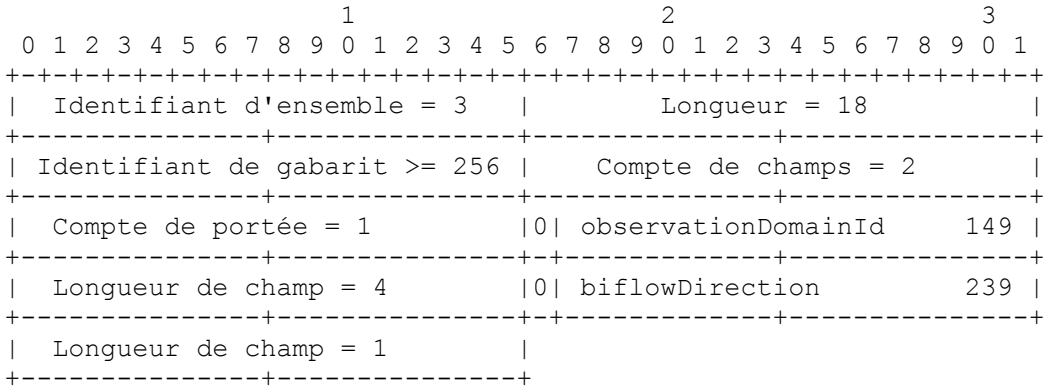


Figure 9 : Ensemble de gabarit d'options biflowDirection

L'exemple suivant d'ensemble de données spécifierait que le choix de direction du périmètre est effectué pour le domaine d'observation avec l'identifiant 33. Son format est défini par l'exemple de gabarit d'options ci-dessus. Noter que cet exemple d'ensemble de données serait envoyé de façon fiable, comme spécifié dans la description de l'élément d'information biflowDirection.

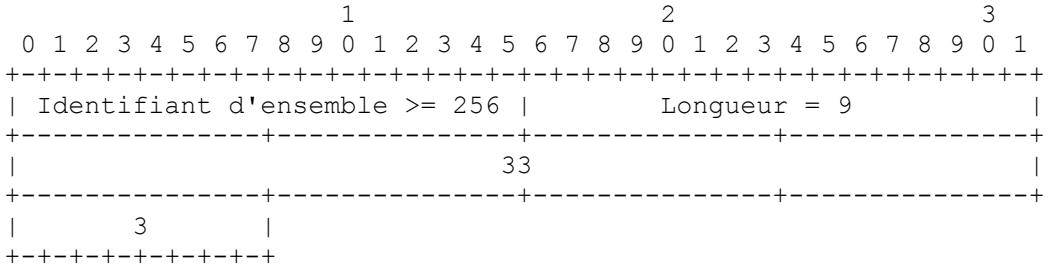


Figure 10 : Ensemble de données d'options biflowDirection

Appendice B. Spécification XML de l'élément d'information biflowDirection

Cet appendice contient une description lisible par la machine de l'élément d'information biflowDirection défini dans le présent document, codée en XML. Noter que cet appendice est de nature informative, alors que le texte du paragraphe 6.3 est normatif.

Le format dans lequel est donnée cette spécification est décrit par le schéma XML de l'Appendice B du modèle d'information IPFIX [RFC5102].

```
  <?xml version="1.0" encoding="UTF-8"?>

<fieldDefinitions xmlns="urn:ietf:params:xml:ns:ipfix-info"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:schemaLocation="urn:ietf:params:xml:ns:ipfix-info ipfix-info.xsd">

<field name="biflowDirection" dataType="unsigned8"
      dataTypeSemantics="identifier" group="misc"
      elementId="239" applicability="all" status="current">
   <description>
    <paragraph>
    Description de la méthode d'allocation de direction utilisée pour allouer la source et destination de biflux. Cet élément
    d'information PEUT être présent dans un enregistrement de données de flux, ou appliqué à tous les flux exportés d'un
    processus d'exportation ou domaine d'observation utilisant les options IPFIX. Si cet élément d'information n'est pas
    présent dans un enregistrement de flux ou associé à un biflux via une portée, on suppose que la configuration de la
    méthode d'allocation de direction est faite hors bande. Noter que quand on utilise les options IPFIX pour appliquer cet
    élément d'information à tous les flux dans un domaine d'observation ou provenant d'un processus d'exportation, l'option
    DEVRAIT être envyée de façon fiable. Si un transport fiable n'est pas disponible (c'est-à-dire, quand on utilise UDP)
    cet élément d'information DEVRAIT apparaître dans chaque enregistrement de flux. Ce champ peut prendre les valeurs
    suivantes :
    </paragraph>
    <artwork>
```

Valeur	Nom	Description
0x00	arbitraire	La direction allouée est arbitraire.
0x01	initiateur	La source de biflux est le flux initiateur, comme déterminé par le mieux que peut faire le processus de mesure pour détecter l'initiateur.
0x02	reverseInitiator	La destination du biflux est le flux initiateur, comme déterminé par le mieux que peut faire le processus de mesure pour détecter l'initiateur. Cette valeur est fournie pour l'agrément du processus exportateur pour réviser l'estimation d'un initiateur sans re-coder l'enregistrement de biflux.
0x03	périmètre	La source de biflux est le point d'extrémité en-dehors d'un périmètre défini. La définition du périmètre est implicite dans l'ensemble des adresses de source de biflux et de destination de biflux exporté dans les enregistrements de biflux.

```
    </artwork>
   </description>
  </field>
</fieldDefinitions>
```

Adresse des auteurs

Brian H. Trammell
CERT Network Situational Awareness
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213
United States
téléphone : +1 412 268 9748
mél : bht@cert.org

Elisa Boschi
Hitachi Europe
c/o ETH Zurich
Gloriastrasse 35
8092 Zurich
Switzerland
téléphone : +41 44 6327057
mél : elisa.boschi@hitachi-eu.com

Déclaration complète de droits de reproduction