

Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.2770

(11/2012)

SÉRIE Y: INFRASTRUCTURE MONDIALE DE
L'INFORMATION, PROTOCOLE INTERNET ET
RÉSEAUX DE PROCHAINE GÉNÉRATION

Réseaux de prochaine génération – Sécurité

**Spécifications relatives au contrôle approfondi
des paquets dans les réseaux de prochaine
génération**

Recommandation UIT-T Y.2770



RECOMMANDATIONS UIT-T DE LA SÉRIE Y
**INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE
PROCHAINE GÉNÉRATION**

INFRASTRUCTURE MONDIALE DE L'INFORMATION	
Généralités	Y.100–Y.199
Services, applications et intergiciels	Y.200–Y.299
Aspects réseau	Y.300–Y.399
Interfaces et protocoles	Y.400–Y.499
Numérotage, adressage et dénomination	Y.500–Y.599
Gestion, exploitation et maintenance	Y.600–Y.699
Sécurité	Y.700–Y.799
Performances	Y.800–Y.899
ASPECTS RELATIFS AU PROTOCOLE INTERNET	
Généralités	Y.1000–Y.1099
Services et applications	Y.1100–Y.1199
Architecture, accès, capacités de réseau et gestion des ressources	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interfonctionnement	Y.1400–Y.1499
Qualité de service et performances de réseau	Y.1500–Y.1599
Signalisation	Y.1600–Y.1699
Gestion, exploitation et maintenance	Y.1700–Y.1799
Taxation	Y.1800–Y.1899
Télévision IP sur réseaux de prochaine génération	Y.1900–Y.1999
RÉSEAUX DE PROCHAINE GÉNÉRATION	
Cadre général et modèles architecturaux fonctionnels	Y.2000–Y.2099
Qualité de service et performances	Y.2100–Y.2199
Aspects relatifs aux services: capacités et architecture des services	Y.2200–Y.2249
Aspects relatifs aux services: interopérabilité des services et réseaux dans les réseaux de prochaine génération	Y.2250–Y.2299
	Y.2300–Y.2399
Gestion de réseau	Y.2400–Y.2499
Architectures et protocoles de commande de réseau	Y.2500–Y.2599
Réseaux de transmission par paquets	Y.2600–Y.2699
Sécurité	Y.2700–Y.2799
Mobilité généralisée	Y.2800–Y.2899
Environnement ouvert de qualité opérateur	Y.2900–Y.2999
RÉSEAUX FUTURS	Y.3000–Y.3499
INFORMATIQUE EN NUAGE	Y.3500–Y.3999

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T Y.2770

Spécifications relatives au contrôle approfondi des paquets dans les réseaux de prochaine génération

Résumé

La Recommandation UIT-T Y.2770 contient les spécifications relatives au contrôle approfondi des paquets (DPI, *deep packet inspection*) dans les réseaux de prochaine génération (NGN, *next generation network*). Elle détaille avant tout les spécifications qui concernent les entités du contrôle approfondi des paquets (entités DPI) dans les réseaux NGN, traitant en particulier des aspects tels que l'identification des applications, l'identification des flux, les types de trafic contrôlés, la gestion des signatures, la communication de données au système de gestion du réseau (NMS, *network management system*) et l'interaction avec l'entité fonctionnelle chargée des décisions en matière de politique. Bien que s'adressant principalement aux réseaux NGN, les spécifications peuvent s'appliquer à d'autres types de réseaux.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T Y.2770	2012-11-20	13

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous <http://www.itu.int/ITU-T/ipr/>.

© UIT 2013

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

	Page
1	Domaine d'application 1
1.1	Applicabilité 1
1.2	Règles de politique 2
2	Références..... 3
3	Définitions 4
3.1	Termes définis ailleurs 4
3.2	Termes définis dans la présente Recommandation 5
4	Abréviations et acronymes 8
5	Conventions 9
6	Spécifications relatives aux entités fonctionnelles DPI..... 10
6.1	Identification du flux et de l'application..... 10
6.2	Gestion des signatures DPI..... 10
6.3	Aspects concernant le contrôle du trafic 12
6.4	Communication de données 16
6.5	Interaction avec une fonction de décision en matière de politique 18
6.6	Commande du trafic 19
6.7	Identification de la session 19
6.8	Contrôle du trafic chiffré 19
6.9	Contrôle du trafic comprimé 21
6.10	Détection d'un trafic anormal 21
7	Spécifications fonctionnelles du point de vue du réseau 22
7.1	Spécifications générales 22
7.2	Plan de données, plan de commande et plan de gestion dans un nœud DPI.. 22
8	Interfaces de l'entité fonctionnelle DPI 24
8.1	Interfaces externes de l'entité fonctionnelle DPI..... 25
8.2	Interfaces internes de l'entité DPI-FE..... 25
8.3	Spécifications relatives aux interfaces..... 26
9	Considérations et spécifications en matière de sécurité 26
9.1	Menaces pour la sécurité des entités DPI 26
9.2	Spécifications en matière de sécurité pour les entités DPI..... 27
	Annexe A – Spécification d'un descripteur de flux 28
A.1	Point de vue syntaxique du protocole..... 28
A.2	Spécification des valeurs des éléments d'information 29
A.3	Relation entre un descripteur de flux, un identificateur de flux IPFIX et une clé de flux IPFIX 29
	Bibliographie..... 31

Recommandation UIT-T Y.2770

Spécifications relatives au contrôle approfondi des paquets dans les réseaux de prochaine génération

1 Domaine d'application

La présente Recommandation détaille avant tout les spécifications qui concernent les entités du contrôle approfondi des paquets (DPI, *deep packet inspection*) dans les réseaux de prochaine génération (NGN, *next generation network*), traitant en particulier des aspects tels que l'identification des applications, l'identification des flux, les types de trafic contrôlés, la gestion des signatures, la communication de données au système de gestion du réseau (NMS, *network management system*) et l'interaction avec l'entité fonctionnelle chargée des décisions en matière de politique.

Elle contient aussi les spécifications relatives au contrôle DPI du trafic dans des formats de codage non natifs (par exemple, le trafic chiffré, les données comprimées et les informations transcodées).

Toute fonction DPI peut en général être décrite au moyen de la notion de règles de politique (voir le § 1.2).

Les responsables chargés de la mise en œuvre et les utilisateurs des techniques décrites doivent se conformer à l'ensemble des lois, des règlements et des politiques applicables aux niveaux national et régional. Le mécanisme décrit dans la présente Recommandation pourra ne pas s'appliquer aux correspondances internationales afin d'en assurer le secret et de respecter les dispositions juridiques nationales en matière de souveraineté pour ce qui est des télécommunications et les dispositions de la Constitution et de la Convention de l'UIT.

La présente Recommandation n'aborde pas les effets particuliers qui découlent de l'exécution d'une fonctionnalité DPI répartie. Les spécifications concernent essentiellement les aspects fonctionnels du contrôle DPI, mais les aspects physiques y sont aussi abordés. S'agissant des scénarios de mappage d'entités fonctionnelles sur des entités physiques, seuls sont examinés dans le cadre de la présente Recommandation les mappages d'une entité fonctionnelle DPI (DPI-FE, *DPI functional entity*) sur une entité physique DPI (DPI-PE, *DPI physical entity*) et ceux de N entités DPI-FE sur une entité DPI-PE. En d'autres termes, aucune spécification ne concerne les entités DPI-FE réparties.

1.1 Applicabilité

La présente Recommandation s'applique aux scénarios indiqués dans la Figure 1-1:

		Type de réseau en mode paquet	
		Réseau NGN	Réseau non NGN
Technologie de support en mode paquet	IP	Applicable	Eventuellement applicable
	Non IP	Eventuellement applicable	Eventuellement applicable

Y.2770(12)_F1-1

Figure 1-1 – Applicabilité de la présente Recommandation

La notion "non IP" (IP, *Internet protocol*) renvoie aux piles de protocoles des types de support en mode paquet sans couche de protocole IP (références [IETF RFC 791] et [IETF RFC 2460]).

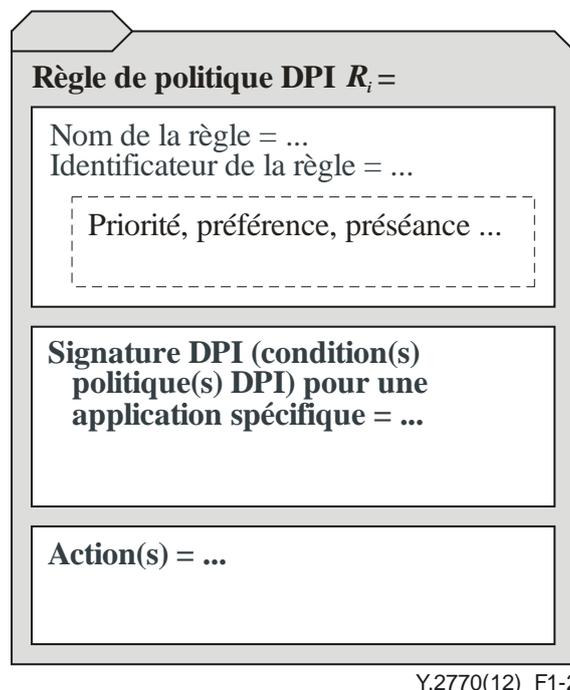
Bien que la présente Recommandation traite principalement des spécifications relatives au contrôle DPI dans les réseaux NGN, ces spécifications peuvent s'appliquer à d'autres types de réseaux. Ces autres applications doivent faire l'objet d'un complément d'étude.

1.2 Règles de politique

Dans la présente Recommandation, on suppose un format générique de haut niveau pour toutes les règles de politique. Ce format de haut niveau s'applique aux règles de contrôle DPI, comme indiqué dans la Figure 1-2. Le format prévoit les trois blocs fondamentaux suivants:

- i) l'identificateur ou le nom des règles (accompagné d'une indication de rang ou d'ordre, dans l'éventualité de règles multiples);
- ii) la signature ou les conditions DPI;
- iii) les actions.

Il existe un lien logique entre la ou les actions et la ou les conditions (voir le § 3.1.2).



Y.2770(12)_F1-2

Figure 1-2 – Format générique des règles de politique DPI

Il convient de noter que les aspects suivants entrent dans le cadre de la présente Recommandation:

- la spécification des prescriptions relatives à la signature DPI (par exemple, les signatures DPI employées pour l'identification des applications et l'identification des flux);
- la spécification des prescriptions relatives à l'identification et à la dénomination des règles de politique DPI;
- l'identification des scénarios possibles faisant appel à des actions politiques telles que des activités éventuelles de suivi après l'évaluation des signatures DPI.

Par contre, les aspects suivants sortent du cadre de la présente Recommandation:

- la spécification des prescriptions relatives aux actions visant à modifier le ou les paquets contrôlés;
- la spécification des relations explicites entre les actions et les conditions (Note);
- la spécification complète des règles de politique DPI;
- la spécification d'un langage pour les signatures DPI;
- la spécification des conditions politiques DPI concrètes (telles que les fonctions comportementales ou statistiques).

NOTE – Par exemple, il pourrait y avoir une spécification relative à l'action consistant à rejeter un paquet, et une spécification de la condition de la recherche d'une signature de paquet, mais il n'y aura pas de spécification qui associe une action individuelle à une condition réelle.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

- [UIT-T E.107] Recommandation UIT-T E.107 (2007), *Service de télécommunications d'urgence (ETS) et cadre d'interconnexion des mises en œuvre nationales du service ETS*.
- [UIT-T X.200] Recommandation UIT-T X.200 (1994) | ISO/CEI 7498-1:1994, *Technologies de l'information – Interconnexion des systèmes ouverts – Modèle de référence de base: le modèle de référence de base*.
- [UIT-T X.731] Recommandation UIT-T X.731 (1992) | ISO/CEI 10164-2:1993, *Technologies de l'information – Interconnexion des systèmes ouverts – Gestion-systèmes: fonction de gestion d'états*.
- [UIT-T Y.1221] Recommandation UIT-T Y.1221 (2010), *Gestion du trafic et des encombrements dans les réseaux en mode IP*.
- [UIT-T Y.2111] Recommandation UIT-T Y.2111 (2008), *Fonctions de commande de ressource et d'admission dans les réseaux de prochaine génération*.
- [UIT-T Y.2205] Recommandation UIT-T Y. 2205 (2011), *Réseaux de prochaine génération – Télécommunications d'urgence – Considérations techniques*.
- [UIT-T Y.2701] Recommandation UIT-T Y.2701 (2007), *Prescriptions de sécurité des réseaux de prochaine génération de version 1*.
- [UIT-T Y.2704] Recommandation UIT-T Y.2704 (2010), *Mécanismes et procédures de sécurité applicables aux réseaux de prochaine génération*.
- [IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol*.
- [IETF RFC 2460] IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6) Spécification*.
- [IETF RFC 5101] IETF RFC 5101 (2008), *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation emploie les termes suivants définis ailleurs:

3.1.1 filtre [b-IETF RFC 3198]: un ensemble de termes et/ou de critères employés à des fins de séparation ou de classement. Cela se fait au moyen de la mise en concordance, pour un champ unique ou des champs multiples, de l'en-tête de trafic et/ou des données utiles. Des "filtres" sont souvent manipulés et employés lors de l'exploitation du réseau et de la mise en application des politiques. Par exemple, les filtres de paquets spécifient les critères pour la mise en concordance avec une configuration (par exemple, des critères IP ou 802) en vue de différencier les classes distinctes de trafic.

NOTE – Dans la présente Recommandation, le terme "en-tête de trafic" est équivalent au terme "en-tête de paquet".

3.1.2 règle de filtre ou de politique [b-IETF RFC 3198]: un module de base d'un système fondé sur les politiques. Il s'agit du lien entre un ensemble d'actions et un ensemble de conditions, ces dernières étant évaluées pour déterminer si les actions seront exécutées.

NOTE – Dans la présente Recommandation, une règle de filtre est une règle de politique particulière qui a pour objet de séparer le trafic, par exemple, dans les grandes catégories de "trafic accepté" et de "trafic non accepté".

3.1.3 flux [IETF RFC 5101]: un ensemble de paquets IP passant par un point d'observation dans le réseau pendant un certain intervalle de temps. Tous les paquets appartenant à un flux donné ont un ensemble de propriétés communes. Chacune des propriétés est définie comme le résultat de l'application d'une fonction aux valeurs:

- 1) De l'un ou de plusieurs champs d'en-tête de paquet (par exemple, l'adresse IP de destination), champs d'en-tête de transport (par exemple, le numéro du port de destination) ou champs d'en-tête d'application (par exemple, les champs d'en-tête du protocole en temps réel (RTP, *real time protocol*) [b-IETF RFC 3550]).
- 2) De l'une ou de plusieurs caractéristiques du paquet lui-même (par exemple, le numéro des étiquettes de la commutation multiprotocole avec étiquette (MPLS, *multiprotocol label switching*), etc.).
- 3) De l'un ou de plusieurs champs obtenus lors du traitement du paquet (par exemple, l'adresse IP du prochain saut, l'interface de sortie).

Par définition, un paquet appartient à un flux s'il satisfait intégralement à toutes les propriétés définies du flux.

Cette définition couvre la gamme de flux allant d'un flux contenant tous les paquets observés à une interface de réseau à un flux ne comportant qu'un seul paquet entre deux applications. Elle inclut les paquets sélectionnés au moyen d'un processus d'échantillonnage.

NOTE – Les alinéas ci-dessus concernent les propriétés du flux dans les catégories 1) des "informations de commande de protocole (PCI, *protocol command information*) des paquets", 2) des "propriétés des unités de données de protocole (PDU, *protocol data unit*) des paquets" et 3) des "informations locales de transmission des paquets".

3.1.4 politique [b-IETF RFC 3198]: un ensemble de règles permettant d'administrer, de gérer et de commander l'accès aux ressources du réseau.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 **application**: un des éléments suivants:

- *Un type de protocole d'application* (par exemple, les protocoles d'application IP UIT-T H.264 vidéo ou le protocole d'ouverture de session (SIP, *session initiation protocol*)).
- *Une instance d'utilisateur desservi* (par exemple, VoIP, VoLTE, VoIMS, VoNGN ou VoP2P) d'un type d'application, par exemple l'"application voix sur paquets".
- *Une "application propre à un fournisseur"* pour la transmission de la voix sur paquets (par exemple, VoIP par un fournisseur 3GPP, VoIP par Skype).
- *Une application incorporée dans une autre application* (par exemple, un contenu d'application dans un élément du corps d'un message de protocole SIP ou de transfert hypertexte (HTTP, *hypertext transfer protocol*)).

Une application est identifiable par un identificateur particulier (par exemple, au moyen d'un champ binaire, d'une configuration, d'une signature ou d'une expression régulière telle que les "conditions au niveau de l'application", voir le § 3.2.2), qui est une caractéristique commune à tous les niveaux d'application énumérés ci-dessus.

3.2.2 **descripteur d'application (aussi nommé conditions au niveau de l'application)**: un ensemble de conditions réglementaires qui identifient l'application (conformément au § 3.2.1).

La présente Recommandation considère le descripteur d'application comme un objet en général, qui est synonyme des conditions au niveau de l'application. Elle n'aborde pas sa structure détaillée, par exemple la syntaxe, le codage et le type de données.

3.2.3 **étiquette d'application**: un nom unique d'application, qui est employé pour indiquer la sémantique de l'application et est généralement utilisé pour les scénarios de communication de données.

Dans la Figure 3-1 est illustrée la relation entre l'étiquette d'application et le descripteur d'application.

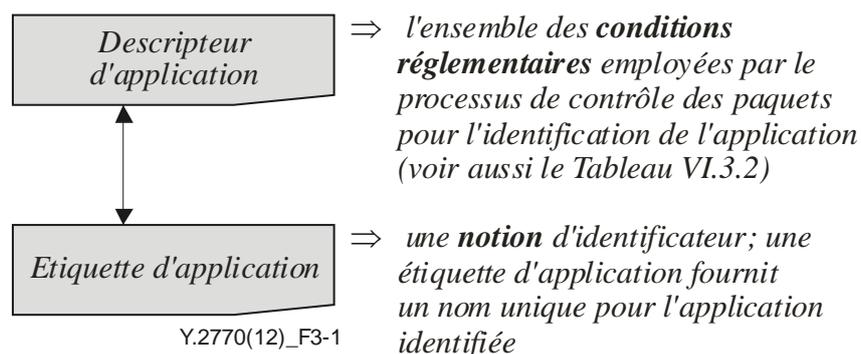


Figure 3-1 – Relation entre l'étiquette d'application et le descripteur d'application

3.2.4 **contrôle DPI bidirectionnel**: un contrôle DPI qui implique des conditions politiques applicables aux deux sens de trafic.

NOTE – Il y a au moins une condition simple par sens de trafic dans le cas d'un contrôle DPI bidirectionnel.

3.2.5 **contrôle approfondi des paquets (DPI)**: une analyse, conforme au modèle de référence de base pour l'interconnexion des systèmes ouverts (OSI-BRM, *open system interconnection basic reference model*) [UIT-T X.200] à architecture de protocole en couches,

- des propriétés des données utiles et/ou des paquets (voir la liste des propriétés possibles au § 3.2.11), en dessous des informations d'en-tête des couches de protocole 2, 3 ou 4 (L2/L3/L4);
- d'autres propriétés des paquets;

afin d'identifier l'application sans ambiguïté.

NOTE – Les informations obtenues par la fonction DPI, assorties de certaines informations supplémentaires comme des informations sur le flux, sont généralement employées par les fonctions suivantes telles que la communication de données et l'exécution d'actions sur le paquet.

3.2.6 moteur DPI: une sous-composante et partie centrale de l'entité fonctionnelle DPI qui exécute toutes les fonctions de traitement sur le trajet des paquets (par exemple, la fonction d'identification des paquets et d'autres fonctions de traitement des paquets de la Figure 6-1).

3.2.7 entité DPI: une entité DPI qui est soit une entité fonctionnelle DPI soit une entité physique DPI.

3.2.8 entité fonctionnelle DPI (DPI-FE): une entité fonctionnelle qui effectue un contrôle approfondi des paquets.

3.2.9 entité physique DPI (DPI-PE): l'instance mise en œuvre d'une entité fonctionnelle DPI.

3.2.10 politique DPI: une politique telle qu'elle est définie dans la référence [b-IETF RFC 3198] (voir le § 3.1.4), appliquée dans une entité DPI.

3.2.11 condition politique DPI (aussi nommée signature DPI): une représentation de l'état et/ou des éléments prérequis nécessaires qui identifient une application et définissent si des actions prévues par une règle de politique doivent être exécutées. L'ensemble des conditions politiques DPI associées à une règle de politique spécifie si la règle de politique est applicable (voir aussi la référence [b-IETF RFC 3198]).

Une condition politique DPI doit contenir des conditions au niveau de l'application et peut contenir d'autres options telles que les conditions concernant l'état et/ou les conditions au niveau du flux:

- 1) Condition concernant l'état (à titre facultatif):
 - a) les conditions concernant le niveau de service dans le réseau (par exemple, l'encombrement rencontré sur le trajet des paquets); ou
 - b) l'état de l'élément de réseau (par exemple, la condition locale de surcharge de l'entité DPI-FE).
- 2) Descripteur du flux ou conditions au niveau du flux (à titre facultatif):
 - a) le contenu des paquets (champs d'en-tête);
 - b) les caractéristiques d'un paquet (par exemple, le nombre d'étiquettes MPLS);
 - c) le traitement des paquets (par exemple, l'interface de sortie de l'entité DPI-FE).
- 3) Descripteur d'application ou conditions au niveau de l'application:
 - a) le contenu des paquets (les champs d'en-tête de l'application et les données utiles de l'application).

NOTE – La condition se rapporte à la "condition simple" dans les descriptions formelles des conditions au niveau du flux et des conditions au niveau de l'application.

3.2.12 entité fonctionnelle DPI chargée des décisions en matière de politique (DPI-PDFE, *policy decision functional entity*): la fonction, éloignée de la fonction DPI-FE, qui décide des règles fondées sur les signatures à appliquer dans l'entité DPI-FE. Certaines fonctions de commande et/ou de gestion ne sont pas nécessairement éloignées de l'entité DPI-FE.

3.2.13 règle de politique DPI: la règle de politique convenant au contrôle DPI (voir aussi le § 3.1.2). Dans la présente Recommandation, une règle de politique DPI est simplement nommée règle.

3.2.14 signature DPI: un synonyme de la ou des conditions politiques DPI (voir le § 3.2.11).

3.2.15 bibliothèque de signatures DPI: une base de données comportant un ensemble de signatures DPI. Elle est aussi nommée bibliothèque de protocoles DPI, parce que les signatures peuvent habituellement être employées pour l'identification des protocoles.

3.2.16 descripteur de flux (aussi nommé conditions au niveau du flux): un ensemble de conditions réglementaires qui est employé pour identifier un type spécifique de flux (conformément au § 3.1.3) à partir du trafic contrôlé.

NOTE 1 – Cette définition de descripteur de flux étend celle qui est donnée dans la référence [b-UIT-T Y.2121] en lui ajoutant des éléments comme décrit au § 3.

NOTE 2 – Pour une analyse normative plus détaillée du descripteur de flux tel qu'il est utilisé dans la présente Recommandation, voir l'Annexe A.

3.2.17 identificateur de flux destiné à l'exportation d'informations sur les flux IP (IPFIX, *IP flux information export*): l'ensemble de valeurs pour les clés de flux IPFIX, qui est employé conjointement avec le descripteur de flux pour identifier un flux donné.

3.2.18 clé de flux IPFIX: chacun des éléments d'information du descripteur de flux qui est employé dans les processus d'identification des flux fondés sur l'exportation IPFIX (conformément à la référence [IETF RFC 5101]).

NOTE – La définition de la clé de flux IPFIX est cohérente sur le plan sémantique avec la définition de la clé de flux, donnée dans la procédure d'exportation IPFIX [IETF RFC 5101]. La seule différence entre les deux termes réside dans le fait que la définition dans le présent document est étendue au descripteur de flux.

3.2.19 contrôle d'en-tête au niveau des couches L3,4 ($L_{3,4}HI$, *L_{3,4} header inspection*): l'application de la ou des règles de politique dans le cas de conditions politiques ne comportant que des éléments d'information de commande de protocole (PCI, *protocol control information*) au niveau de la couche réseau et/ou de la couche transport.

3.2.20 contrôle d'en-tête au-dessus de la couche L4 ($L_{4+}HI$): l'application de la ou des règles de politique dans le cas de conditions politiques ne comportant que des éléments PCI au-dessus de la couche transport.

3.2.21 contrôle des données utiles au niveau de la couche L4 (L_4PI , *L₄ payload inspection*): L'application de la ou des règles de politique dans le cas de conditions politiques ne comportant que des données utiles concernant le transport qui peuvent être les "données concernant l'application" pour des protocoles d'application particuliers (par exemple, le protocole SIP).

NOTE – Le contrôle L_4PI intègre les conditions politiques des contrôles $L_{4+}HI$ et L_7PI .

3.2.22 contrôle des données utiles au niveau de la couche L7 (L_7PI): l'application de la ou des règles de politique dans le cas de conditions politiques fondées sur les données concernant l'application.

3.2.23 données utiles: L'unité de données à la suite des éléments de l'en-tête d'un paquet, à l'exclusion des éléments facultatifs à la fin du paquet (par exemple, les éléments de remplissage, les éléments de fin de paquet ou le total de contrôle).

NOTE 1 – Ainsi, la notion de données utiles est synonyme d'unité de données de service (SDU, *service data unit*) dans le modèle OSI-BRM [UIT-T X.200], celle de paquet est synonyme de l'unité de données de protocole (PDU, *protocol data unit*), tandis que celle d'informations de commande de protocole (PCI, *protocol control information*) regroupe tous les éléments d'en-tête de paquet et de fin de paquet. En résumé "PDU = PCI + SDU".

NOTE 2 – La notion de données utiles est propre à une couche particulière de protocole (à savoir, la notion *données utiles Lx* renvoie aux données utiles au niveau de la couche de protocole x). La même chose vaut pour les unités *SDU Lx* et *PDU Lx* et pour les informations *PCI Lx*).

4 Abréviations et acronymes

La présente Recommandation emploie les abréviations et les acronymes suivants:

AH	en-tête d'authentification (<i>authentication header</i>)
BRM	modèle de référence de base (<i>basic reference model</i>)
DCCP	protocole de commande en cas d'encombrement des datagrammes (<i>datagram congestion control protocol</i>)
DPI	contrôle approfondi des paquets (<i>deep packet inspection</i>)
DPI-FE	entité fonctionnelle DPI (<i>DPI functional entity</i>)
DPI-PDFE	entité fonctionnelle DPI chargée des décisions en matière de politique (<i>DPI policy decision functional entity</i>)
DPI-PE	entité physique DPI (<i>DPI physical entity</i>)
DPI-PIB	base d'informations politiques DPI (<i>DPI policy information base</i>)
ESP	données utiles pour la sécurité d'encapsulation (<i>encapsulating security payload</i>)
ET	télécommunications d'urgence (<i>emergency telecommunications</i>)
FPA	analyse complète de la zone des données utiles (<i>full payload area analysis</i>)
FSL	langage de spécification du filtre (<i>filter specification language</i>)
HTTP	protocole de transfert hypertexte (<i>hypertext transfer protocol</i>)
IANA	Autorité chargée de l'assignation des numéros Internet (Internet assigned numbers Authority)
IE	éléments d'information (<i>information elements</i>)
IP	protocole Internet (<i>Internet protocol</i>)
IPFIX	exportation d'informations sur les flux IP (<i>IP flow information export</i>)
IS	en service (<i>in-service</i>)
L-PDF	fonction PDF locale (<i>local PDF</i>)
MPLS	commutation multiprotocole avec étiquette (<i>multi protocol label switching</i>)
NGN	réseau de prochaine génération (<i>next generation network</i>)
NMS	système de gestion de réseau (<i>network management system</i>)
OGP	protocole ouvert pour les jeux (<i>open game protocol</i>)
OoS	hors service (<i>out-of-service</i>)
OSI-BRM	modèle de référence de base pour l'interconnexion des systèmes ouverts (<i>open systems interconnection – basic reference model</i>)
P2P	homologue à homologue (<i>peer to peer</i>)
PCC	commande des politiques et de la taxation (<i>policy and charging control</i>)
PCI	informations de commande de protocole (<i>protocol control information</i>)
PDF	fonction de décision en matière de politique (<i>policy decision function</i>)

PDU	unité de données de protocole (<i>protocol data unit</i>)
PEL	langage d'expression des politiques (<i>policy expression language</i>)
PPF	fonction de transmission des paquets (<i>packet forwarding function</i>)
PIB	base d'informations politiques (<i>policy information base</i>)
PPA	analyse de la zone des données utiles (<i>payload area analysis</i>)
PSAMP	échantillonnage de paquets (<i>packet sampling</i>)
PSL	langage de spécification des politiques (<i>policy specification language</i>)
RACF	fonction de commande des ressources et de l'admission (<i>resource and admission control function</i>)
RACS	sous-système de commande des ressources et de l'admission (<i>resource and admission control subsystem</i>)
R-PDF	fonction PDF distante (<i>remote PDF</i>) (c'est-à-dire, fonction PDF éloignée du nœud DPI)
RTP	protocole de transport en temps réel (<i>real-time transport protocol</i>)
SA	association de sécurité (<i>security association</i>) (IPsec)
SCTP	protocole de transmission de commande de flux (<i>stream control transmission protocol</i>)
SDU	unité de données de service (<i>service data unit</i>)
SigComp	compression de la signalisation (<i>signalling compression</i>)
SIP	protocole d'ouverture de session (<i>session initiation protocol</i>)
SPI	indice du paramètre de sécurité (<i>security parameter index</i>) (IPsec)
TCP	protocole de commande de transmission (<i>transmission control protocol</i>)
TISPAN	services et protocoles des télécommunications et de l'Internet mis en convergence pour une mise en réseau évoluée (<i>telecommunication and Internet converged services and protocols for advanced networking</i>)
UDP	protocole de datagrammes d'utilisateur (<i>user datagram protocol</i>)

5 Conventions

Le présent document contient une liste de sujets, repérés par la mention *R-x/y*, où *x* est le numéro de § et *y* est un numéro d'ordre au sein de ce paragraphe. Ces sujets font appel aux mots-clés suivants, dont la signification est prescrite ci-après:

Les mots-clés "est obligatoire" indiquent une spécification qui doit rigoureusement être respectée et par rapport à laquelle aucun écart n'est admis pour pouvoir déclarer la conformité au présent document.

Les mots-clés "est interdit" indiquent une spécification qui doit rigoureusement être respectée et par rapport à laquelle aucun écart n'est admis pour pouvoir déclarer la conformité au présent document.

Les mots-clés "est recommandé" indiquent une spécification qui est recommandée mais n'est pas requise de façon absolue. Il ne doit donc pas nécessairement être satisfait à cette spécification pour déclarer la conformité.

Les mots-clés "peut à titre facultatif" indiquent une spécification facultative qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elle ne doit pas être interprétée comme l'obligation pour le fabricant de mettre en œuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de services de l'activer ou non, mais comme la possibilité pour le fabricant de fournir ou non cette option, sans que cela n'ait d'incidence sur la déclaration de conformité.

Dans le corps de la présente Recommandation et dans ses annexes, les mots "doit", "ne doit pas", "devrait" et "peut" sont parfois employés, auxquels cas ils doivent être interprétés, respectivement, comme "est obligatoire", "est interdit", "est recommandé" et "peut à titre facultatif". La présence de telles expressions ou mots-clés dans un appendice ou dans un élément d'information qui porte explicitement la mention "à titre informatif" doit être interprétée comme n'étant pas à caractère normatif.

6 Spécifications relatives aux entités fonctionnelles DPI

6.1 Identification du flux et de l'application

R-6.1/1: L'entité DPI-FE doit procéder à l'identification de l'application.

R-6.1/2: L'entité DPI-FE doit prendre en charge divers types de règles de politique DPI.

R-6.1/3: L'entité DPI-FE doit identifier une application en contrôlant les données utiles de celle-ci.

R-6.1/4: Les conditions DPI au niveau de l'application (et les conditions facultatives au niveau du flux) doivent permettre l'identification de l'application sur la base du trafic unidirectionnel (contrôle DPI unidirectionnel) pour toutes les applications unidirectionnelles et, sous réserve qu'un sens du trafic permette une identification non ambiguë, pour les applications bidirectionnelles.

R-6.1/5: Les conditions DPI au niveau de l'application (et les conditions facultatives au niveau du flux) peuvent à titre facultatif permettre l'identification de l'application sur la base du trafic bidirectionnel (contrôle DPI bidirectionnel).

R-6.1/6: Il est recommandé que l'élément ou les éléments d'information employés dans les conditions au niveau du flux satisfassent à la référence [b-IETF RFC 5102], telle qu'elle a été enregistrée auprès de l'Autorité IANA [b-IETF IANA IPFIX]. Dans ce cas, il est recommandé que les éléments d'information incluent les éléments d'information IPFIX se rapportant aux couches liaison (L2), réseau (L3) et transport (L4), en suivant l'architecture de protocole en couches de l'IETF de base.

NOTE – Le registre de l'autorité IANA contenant les éléments d'information IPFIX peut à titre facultatif être complété de manière à inclure des éléments supplémentaires (de l'IETF). Le registre actuel de l'Autorité IANA (tel qu'il était à la fin de l'année 2011) manque d'éléments d'information pour les protocoles de la couche L4, autres que les protocoles UDP et TCP (par exemple, les protocoles SCTP et DCCP).

R-6.1/7: L'élément ou les éléments d'information peuvent à titre facultatif être d'autres éléments d'information se rapportant aux couches L2, L3 ou L4, non inclus dans le registre IPFIX (et nommés éléments d'information propres aux entreprises dans le protocole IPFIX [IETF RFC 5101]).

6.2 Gestion des signatures DPI

Le présent paragraphe définit les spécifications relatives aux opérations effectuées dans la bibliothèque de signatures DPI. Ces opérations peuvent être lancées localement par l'entité DPI-FE, ou par une entité de réseau distante (voir la Figure 6-1). Tous les types possibles d'entités de réseau distantes peuvent jouer le rôle de l'entité fonctionnelle DPI chargée des décisions en matière de politique, qui décide des règles fondées sur les signatures à appliquer dans l'entité DPI-FE.

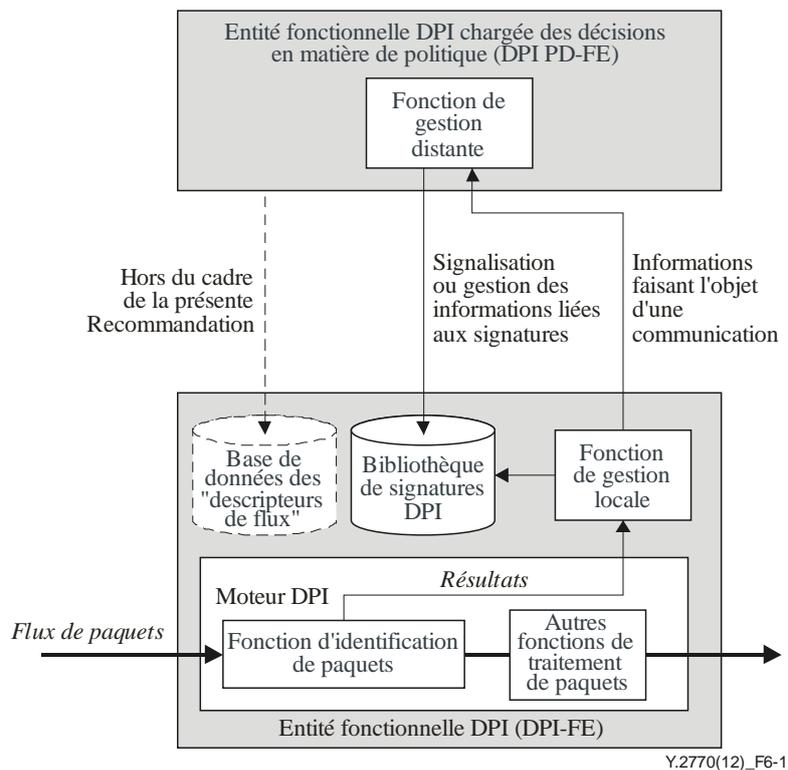


Figure 6-1 – Gestion des signatures DPI dans un exemple d'architecture d'entité fonctionnelle DPI (voir aussi la Figure 8-2 en ce qui concerne les interfaces internes)

L'entité fonctionnelle DPI chargée des décisions en matière de politique doit être associée avec la fonction RACF (dans le cas où le réseau NGN en comporte), mais sa spécification sort du cadre de la présente Recommandation. Elle est présente dans la Figure 6-1 parce qu'elle contient les fonctions de gestion distantes pour l'entité DPI-FE.

6.2.1 Spécifications générales relatives aux signatures

R-6.2.1/1: Les signatures DPI doivent être enregistrées dans la *bibliothèque de signatures DPI* qui est une sous-entité de l'entité DPI-FE.

NOTE – La raison d'être d'une bibliothèque locale de signatures DPI est le fait que la fonction d'identification de paquets nécessite un accès immédiat au contenu de la base de données.

La signature DPI peut être employée:

- pour une identification approximative (par exemple, comportementale, heuristique, etc.);
- pour une identification exacte (par exemple, règles de concordance exacte).

Le langage (formel ou comportemental) employé pour spécifier les règles de politique DPI dans cette bibliothèque, ainsi que les règles de concordance elles-mêmes, sortent du cadre de la présente Recommandation. Celle-ci précise seulement que la bibliothèque existe, ce que sont la ou les signatures DPI et les fonctions de gestion de la bibliothèque.

R-6.2.1/2: La bibliothèque de signatures DPI doit être conservée en lieux sûrs et ne pas être visible par des utilisateurs non autorisés.

6.2.2 Gestion d'une bibliothèque de signatures DPI

Le présent paragraphe définit les spécifications relatives à la gestion d'une bibliothèque de signatures DPI.

6.2.2.1 Adjonction de nouvelles signatures

R-6.2.2.1/1: Il doit être possible d'ajouter de nouvelles signatures DPI à la bibliothèque de signatures DPI.

6.2.2.2 Opérations sur les signatures existantes

R-6.2.2.2/1: Il doit être possible de modifier (mettre à jour) les signatures existantes dans la bibliothèque de signatures DPI.

R-6.2.2.2/2: Il doit être possible d'activer et de désactiver des signatures DPI spécifiques dans la bibliothèque de signatures DPI.

R-6.2.2.2/3: Il doit être possible de supprimer (enlever) des signatures DPI spécifiques dans la bibliothèque de signatures DPI.

6.2.2.3 Format de règles échangé par l'intermédiaire d'interfaces externes

R-6.2.2.3/1: La signature DPI pour l'identification de l'application, échangée par l'intermédiaire d'interfaces externes (c'est-à-dire $e1$ et $e2$ dans la Figure 8-1), peut à titre facultatif avoir un quelconque format de règles (voir aussi le § 1.2).

6.2.3 Emplacement de la fonction de gestion

R-6.2.3/1: Les actions de gestion des signatures DPI spécifiées dans le § 6.2.2 doivent être exécutées localement à partir de l'entité fonctionnelle DPI ou à distance ou des deux manières (voir la Figure 6-1).

6.2.4 Lancement des actions de gestion

R-6.2.4/1: Il est obligatoire de prendre en charge le mode "push" (distribution), s'agissant des opérations de signatures DPI, lorsque les opérations sont lancées à distance (par exemple, par l'entité DPI-PDFE dans la Figure 6-1).

R-6.2.4/2: Il est obligatoire de prendre en charge le mode "pull" (récupération), s'agissant des opérations de signatures DPI, lorsque les opérations sont lancées localement par l'entité DPI-FE. La notion de récupération signifie que la fonction de gestion locale de l'entité DPI-FE demande à l'entité DPI-PDFE d'exécuter une action de gestion concernant une nouvelle signature ou une signature existante.

La façon dont l'entité DPI-FE lance une demande sort du cadre de la présente Recommandation.

6.3 Aspects concernant le contrôle du trafic

Le présent paragraphe porte sur les aspects qui concernent le trafic soumis au contrôle DPI.

6.3.1 Aspects concernant l'identification des flux

R-6.3.1/1: Il est recommandé que l'entité fonctionnelle DPI assure l'identification des applications, sans contrôle au niveau du flux.

R-6.3.1/2: Tout scénario DPI peut à titre facultatif être initialement indépendant du flux, c'est-à-dire que la règle de politique DPI fournie à l'entité DPI-FE ne contient pas de descripteur de flux. Toutefois, la règle peut exiger la collecte d'informations sur le flux concerné.

R-6.3.1/3: Une telle exigence est obligatoire pour fournir une clé de flux IPFIX, ainsi que la restitution facultative des informations manquantes sur les flux.

R-6.3.1/4: L'entité fonctionnelle DPI peut exiger à titre facultatif la reconnaissance complète de l'identificateur de flux IPFIX sur la base d'une clé de flux donnée et le contrôle d'un certain nombre de paquets suivants.

R-6.3.1/5: La communication, par l'entité DPI-FE à une entité de réseau distante, d'un identificateur IPFIX complet ou incomplet peut à titre facultatif être conditionnelle (par exemple, dépendre des événements, être commandée par un temporisateur, etc.).

6.3.2 Aspects concernant le contrôle DPI où sont reconnues ou non reconnues les piles de protocoles

La fonction d'identification DPI (dans l'entité DPI-FE), chargée de l'identification de l'application, concerne les opérations de comparaison et de recherche, fondées sur la signature DPI et effectuées sur un paquet entrant (unité PDU). Il y a deux possibilités: soit l'entité DPI-FE reconnaît la structure interne de l'unité PDU ("*unité DPI-FE reconnaissant les piles de protocoles*"), soit elle ne la reconnaît pas ("*unité DPI-FE ne reconnaissant pas les piles de protocoles*").

Les deux possibilités peuvent conduire à la même identification et être équivalentes sur le plan fonctionnel. La principale différence est que la logique de l'identification où sont reconnues les piles de protocoles peut être plus efficace.

Il est utile de distinguer les deux types d'analyse du point de vue de l'efficacité sur le plan opérationnel (c'est-à-dire l'identification de l'application et l'identification facultative du flux):

- a) Analyse prédéterminée de la zone des données utiles (PPA): Lorsque les paquets (flux) correspondent à une application connue ayant une structure des données utiles clairement définie, l'entité DPI-FE peut contrôler l'emplacement prédéterminé fixé des données utiles (mode de contrôle des paquets où sont reconnues les piles de protocoles).
- b) Analyse complète de la zone des données utiles (FPA): Lorsque les paquets (flux) ne correspondent pas à une application connue ou que la structure des données utiles de l'application n'est pas clairement définie ni connue, l'entité DPI-FE contrôle la "zone entière des données utiles" (mode de contrôle des paquets où ne sont pas reconnues les piles de protocoles).

Le même flux de trafic peut faire l'objet tant de l'analyse PPA que de l'analyse FPA.

R-6.3.2/1: Il est recommandé que l'entité DPI-FE prenne en charge l'identification de l'application où sont reconnues les piles de protocoles.

R-6.3.2/2: Il est recommandé que l'entité DPI-FE prenne en charge l'identification de l'application où ne sont pas reconnues les piles de protocoles.

R-6.3.2/3: L'entité DPI-FE doit identifier les applications exécutées sur les piles de protocoles IPv4 et IPv6 et peut à titre facultatif identifier les applications exécutées sur d'autres piles de protocoles sous-jacentes.

R-6.3.2/4: Il est recommandé que l'entité DPI-FE identifie les applications dans un trafic imbriqué, tel que le trafic encapsulé ou le trafic en tunnel.

6.3.3 Aspects concernant les actions politiques DPI

6.3.3.1 Généralités

Les actions politiques DPI peuvent être exécutées à des niveaux hiérarchiques différents, par exemple au niveau de l'entité DPI-FE ou au niveau des fonctions PDF locales ou distantes, et peuvent par exemple comprendre les actions suivantes:

- 1) Actions au niveau du trajet des paquets (par l'entité DPI-FE):
 - a) accepter le paquet et le transmettre à la fonction de transmission des paquets (PFF) (une action conditionnée pour le mode "contrôle DPI sur le trajet" seulement);

- b) rejeter le paquet (sans notification ou autrement);
 - c) rediriger le paquet vers d'autres interfaces de sortie;
 - d) reproduire le paquet ou créer un paquet miroir destiné aux interfaces de sortie;
 - e) classer le trafic, effectuer les mesures à l'échelle locale et communiquer les données mesurées;
 - f) hiérarchiser, bloquer, conformer et ordonnancer des paquets individuels.
- 2) Actions au niveau des nœuds (impliquant la fonction locale de décision en matière de politique (L-PDF)):
- a) construire dynamiquement des règles de politique DPI et/ou modifier les règles existantes (enregistrées dans la base d'informations politiques DPI (DPI-PIB));
 - b) produire un journal ou des données de suivi et les communiquer à la gestion des politiques (voir le § 2.11.2 de la référence [b-IETF RFC 3871]);
 - c) détecter et communiquer les applications non identifiables;
 - d) notifier les systèmes de détection par intrusion (par exemple, en communiquant des échantillons de trafic, des paquets suspects).
- 3) Actions au niveau du réseau (impliquant la fonction distante de décision en matière de politique (R-PDF)):
- a) gérer les ressources, commander l'admission et filtrer à un haut niveau (au niveau des sous-systèmes de réseau (tels que ceux qui sont spécifiés pour la fonction RACF dans la référence [UIT-T Y.2111], le sous-système RACS des services TISPAN de l'ETSI [b-ETSI ES 282 003] et la commande PCC du projet 3GPP [b-ETSI TS 123 203]));
 - b) taxer les contenus sur la base des types d'application des abonnés (par exemple, RADIUS ou Diameter de l'IETF).

La Figure 6-2 explique plus avant le principe de structure ci-dessus au moyen d'un format générique détaillé des règles de politique (à comparer avec celui qui a été introduit dans le § 1.2):

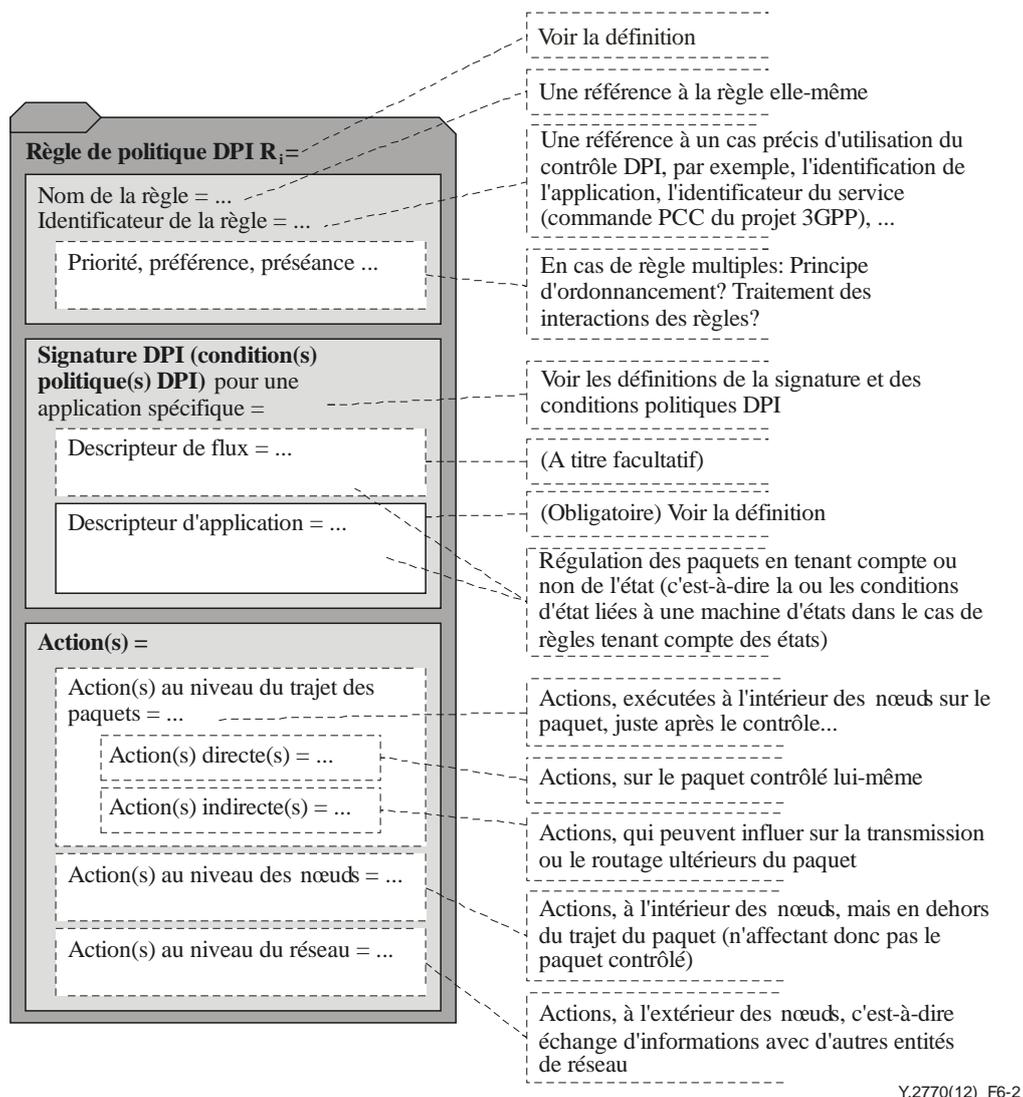


Figure 6-2 – Exemple de format détaillé des règles de politique (à comparer avec celui de la Figure 1-2)

Le mappage des actions spécifiques sur les conditions sort du cadre de la présente Recommandation.

6.3.3.2 Spécifications

R-6.3.3.2/1: Lorsqu'une application a été identifiée par l'entité DPI-FE, on peut, à titre facultatif, extraire des informations propres à l'application.

Par exemple, une adresse URL au format HTTP, un format de média ("type codec") dans le protocole de transport en temps réel (RTP) ou un identificateur de session RTP (par exemple, l'identificateur SSRC pour l'extrémité de la source de synchronisation RTP).

R-6.3.3.2/2: L'entité DPI-FE peut à titre facultatif être en mesure de travailler conjointement avec une fonction de mesure du flux, telle que le processus de mesure IPFIX [IETF RFC 5101] et certaines capacités de filtrage, telles que celles de la référence [b-IETF RFC 5476].

NOTE – Le processus de mesure permet généralement de déterminer les éléments d'information IPFIX suivants (employés comme clés de flux): sourceIPv6Address et destinationIPv6Address, sourceIPv4Address et destinationIPv4Address, protocolIdentifier, sourceTransportPort, destinationTransportPort, etc. Toutefois, il incombe à l'entité DPI-FE de déterminer l'étiquette d'application et la restitution de l'identificateur de flux IPFIX (sur la base de la clé de flux IPFIX donnée, voir aussi la Figure A.1).

6.4 Communication de données

La communication de données consiste en la notification (par exemple, en raison d'un événement particulier détecté par l'entité DPI-FE) à une autre entité fonctionnelle, qui est généralement située dans un élément de réseau distant (dans le plan de l'utilisateur, le plan de commande ou le plan de gestion). L'entité DPI-FE peut employer de multiples interfaces de communication de données à l'appui de "différents types d'événements".

6.4.1 Communication de données au système de gestion du réseau

6.4.1.1 Interface et protocole pour la communication de données

R-6.4.1.1/1: Il est recommandé que le protocole d'exportation satisfasse à la spécification IPFIX [IETF RFC 5101] et puisse à titre facultatif avoir les extensions IPFIX.

R-6.4.1.1/2: Le protocole d'exportation peut à titre facultatif satisfaire à la spécification IPFIX [b-IETF RFC 5103] dans le cas de flux bidirectionnels.

R-6.4.1.1/3: Il est recommandé que les protocoles d'exportation IPFIX emploient l'interface externe e2 (voir la Figure 8-1).

6.4.1.2 Informations communiquées

R-6.4.1.2/1: L'entité DPI-FE doit communiquer au plan de gestion DPI les résultats des contrôles (tels que l'étiquette d'application et les éléments d'information éventuels propres à l'application) ainsi que les informations propres au flux. Les valeurs clés mises à jour localement (notamment les champs typiques de la fonction de mesure de flux) peuvent à titre facultatif être exportées à destination d'une fonction de décision en matière de politique (par exemple, l'entité PD-FE définie dans la référence [UIT-T Y.2111]).

R-6.4.1.2/2: Il est recommandé que les informations communiquées réutilisent les éléments d'information IPFIX ([b-IETF IANA IPFIX]), qui ont initialement été spécifiés dans le modèle d'information IPFIX [b-IETF RFC 5102].

Les informations propres au flux sont spécifiées dans le modèle d'information IPFIX [b-IETF RFC 5102], par exemple:

- 1) des informations propres à l'application:
 - étiquette de l'application;
 - champs extraits tels que le format de média RTP et la source de synchronisation SSRC RTP.
- 2) les champs d'en-tête des couches L3/L4 correspondant aux adresses IP, les ports au niveau de la couche L4 (par exemple, TCP ou UDP, Note 1) et le type de protocole;
- 3) des informations sur la performance (pour la mesure, la statistique): le nombre d'octets, le nombre de paquets et la dimension maximale des paquets (Note 2);
- 4) des informations chronologiques: temps de début du flux, temps de fin du flux;
- 5) des informations associées aux paquets: prochain saut et dimension des paquets (Note 3).

NOTE 1 – Certains des éléments d'information énumérés ne font pas (encore) partie du registre IPFIX de l'autorité IANA, mais ils sont valables dans le cadre de la présente Recommandation.

NOTE 2 – Les informations propres au flux peuvent être produites par un échantillonnage de paquets (PSAMP), mais lors de l'exportation de ces résultats à destination du système NMS, il est recommandé d'ajouter les informations propres à l'application.

NOTE 3 – De nouveaux éléments d'information peuvent devoir être enregistrés auprès de l'autorité IANA IPFIX, conformément au § 7 intitulé "IANA considerations" de la référence [b-IETF RFC 5102].

6.4.2 Communication d'informations sur les applications nouvelles, inconnues ou incorrectes

6.4.2.1 Caractéristiques d'un tel trafic

Les différences entre ces types d'application sont subtiles. Elles peuvent être caractérisées par les propriétés spécifiques suivantes, conduisant à des conditions de détection différentes au niveau de l'application:

- nouvelle application: par exemple, une nouvelle version d'une application, une nouvelle version d'un élément d'information propre à une application (par exemple, une nouvelle version d'un jeu dans le cadre du protocole ouvert pour les jeux (OGP)) ou une nouvelle version de protocole; il convient de noter que la notion de "nouveau" reflète le point de vue du service DPI (qui peut être fondé sur l'historique des services DPI passés);
- application inconnue: par exemple, un type de paquet inconnu, un protocole inconnu, une "application" inconnue;
- application incorrecte: par exemple, un paquet transportant une grammaire de protocole incorrecte (Note), etc.

NOTE – Une syntaxe de protocole incorrecte peut être exploitée pour lancer une attaque compromettant la sécurité. Les protocoles affectés sont généralement ceux qui aboutissent dans l'équipement des utilisateurs (tels que les protocoles de signalisation).

6.4.2.2 Spécifications relatives à la communication de données

R-6.4.2.2/1: L'entité DPI-FE peut à titre facultatif assurer la communication de données sur des applications nouvelles, inconnues ou incorrectes obtenues lors d'un contrôle du trafic.

6.4.3 Communication de données concernant un trafic anormal

R-6.4.3/1: L'entité DPI-FE peut à titre facultatif assurer la communication de données liées à la détection d'un trafic anormal lors du contrôle de ce trafic

Par trafic anormal, on entend un trafic qui n'est pas associé aux classes de trafic normal. Une classe de trafic normal est constituée de trafics dont les propriétés concordent avec des propriétés statistiques existantes d'applications bien définies, telles que le temps entre les arrivées de deux paquets successifs, l'ordre d'arrivée, la dimension de l'unité PDU d'une couche de protocole spécifique, la dimension des données utiles ou le volume de trafic (au niveau d'une couche de protocole spécifique).

6.4.4 Communication de données concernant des événements liés à l'entité physique DPI

Ce paragraphe décrit les événements concernant l'état opérationnel de l'entité DPI et les spécifications relatives à la communication de données.

6.4.4.1 Défaillances liées à un comportement incorrect de l'entité physique DPI

On décrit l'état de gestion de l'entité DPI-PE le plus simplement au moyen de deux états: "en service" (IS) et "hors service" (OoS).

R-6.4.4.1/1: Il est recommandé que la gestion DPI soit fondée sur l'état des connaissances (par exemple, [UIT-T X.731] et [b-IETF RFC 4268]) et prenne en charge au moins les états de gestion en service et hors service.

R-6.4.4.1/2: Toute défaillance de l'entité DPI-PE, si celle-ci n'est pas architecturée de façon redondante, peut éventuellement la faire passer de l'état en service à l'état hors service. Il est recommandé que ces événements soient signalés.

6.4.4.2 Événements liés à la gestion des dérangements par l'entité physique DPI

L'entité DPI-PE fournit les interfaces de réseau pour le trafic d'entrée et de sortie. Des dérangements peuvent se produire au niveau de ces interfaces.

R-6.4.4.2/1: Il est recommandé que l'entité DPI-PE assume la fonction de communication d'une alarme telle que celle définie dans la référence [b-UIT-T X.734].

6.4.4.3 Événements liés à la tenue du journal par l'entité fonctionnelle DPI

R-6.4.4.3/1: L'entité fonctionnelle DPI peut à titre facultatif assurer la tenue d'un journal sur le système comme par exemple le journal Syslog [b-IETF RFC 5424]. Dans ce cas, l'entité fonctionnelle DPI constitue un point d'émission de messages Syslog.

Il convient de noter que dans le cas où le flux de paquets contrôlé achemine le trafic destiné au journal, l'entité fonctionnelle DPI n'est ni un point d'émission ni un point de destination des messages destinés au journal. En d'autres termes, la clé pour la recherche d'un tel flux de paquets peut être fondée sur un descripteur d'application (lié à la couche application syslog) et sur un descripteur de flux IPFIX (liés au mode choisi de transport syslog). Plus d'informations sont données dans les références [b-IETF RFC 5424] et [b-IETF RFC 5426].

6.4.4.4 Événements liés à l'état de charge et à la consommation de ressources par l'entité physique DPI

L'entité DPI-PE dispose de ressources limitées pour l'exécution du contrôle DPI. La spécificité des ressources dépend de la mise en œuvre et sort du cadre de la présente Recommandation.

R-6.4.4.4/1: Il est recommandé que l'entité DPI-PE assure la communication au plan de gestion des données concernant le niveau de charge des composantes ressources DPI.

Par exemple, dans les réseaux acheminant un trafic de télécommunications d'urgence (voir le § 7.1.1), le processus DPI doit être en mesure de transmettre ce trafic à travers les nœuds de réseau encombrés; il est donc souhaitable que le système de gestion du réseau soit au courant du niveau de charge.

6.5 Interaction avec une fonction de décision en matière de politique

R-6.5/1: L'entité DPI-FE peut à titre facultatif jouer le rôle de l'entité fonctionnelle chargée de la mise en application des politiques, comme défini dans la référence [UIT-T Y.2111], et assumer la fonction de transport correspondante.

R-6.5/2: L'interface entre l'entité DPI-FE et la fonction RACF peut à titre facultatif être l'interface *Rw*, comme défini dans la référence [UIT-T Y.2111].

R-6.5/3: Les informations entre l'entité DPI-FE et l'entité PD-FE de la fonction RACF peuvent à titre facultatif être échangées par l'intermédiaire des interfaces existantes (par exemple, l'interface *Rw*) ou nouvelles de la fonction RACF selon le cas précis d'utilisation du contrôle DPI.

NOTE – Dans ce cas, la fonction RACF doit être améliorée pour comporter les informations DPI (par exemple, une signature de protocole dans une règle de politique DPI); la fonction RACF, telle qu'elle est définie dans la référence [UIT-T Y.2111], assure essentiellement l'identification du flux sur la base des règles de politique. Le point de référence particulier de la fonction RACF dépendra du cas précis d'utilisation du contrôle DPI.

6.6 Commande du trafic

Les spécifications de haut niveau suivantes peuvent être déduites:

R-6.6/1: L'entité fonctionnelle DPI peut à titre facultatif être impliquée dans des scénarios de réseau ayant pour but de commander le trafic (par exemple, fonctions de commande du trafic comme définies dans la référence [UIT-T Y.1221]). Il est recommandé que l'entité DPI-FE prenne en charge les capacités de commande du trafic correspondantes.

R-6.6/2: L'entité DPI-FE peut à titre facultatif assurer spontanément la commande du trafic. Mais les spécifications fonctionnelles détaillées de la commande du trafic sortent du cadre de la présente Recommandation.

R-6.6/3: L'entité DPI-FE peut à titre facultatif assurer les interactions avec les fonctions de commande externes. Les spécifications y relatives sortent du cadre de la présente Recommandation.

6.7 Identification de la session

De nombreux termes concernent la session dans la présente Recommandation. L'ensemble du trafic d'une session peut être identifié de façon non ambiguë par l'entité DPI-FE puisque le "descripteur de session" est, soit le même que le descripteur de flux et/ou d'application, soit un sous-ensemble de celui-ci.

6.7.1 Spécifications relatives à la session d'identification

R-6.7.1/1: L'entité DPI-FE doit être en mesure d'analyser le comportement de la session (par exemple, une session RTP, une session HTTP, une session IM ou une session SIP VoIP).

R-6.7.1/2: L'entité DPI-FE doit être en mesure d'assurer le suivi de l'état de la session.

6.7.2 Actions DPI au "niveau de la session"

R-6.7.2/1: L'entité DPI-FE peut à titre facultatif extraire ou produire des données de mesure au niveau de la session (par exemple, pour la surveillance de la mesure de la performance en ce qui concerne la qualité d'expérience de l'utilisateur).

6.8 Contrôle du trafic chiffré

Il est généralement admis que les signatures DPI ne peuvent s'appliquer qu'au trafic non chiffré. Néanmoins, les signatures DPI peuvent s'appliquer au trafic chiffré en fonction:

- du niveau de chiffrement (voir le § 6.8.1);
- de la disponibilité locale de la clé de chiffrement (voir le § 6.8.2);
- des conditions de contrôle sur la base des informations chiffrées (voir le § 6.8.3).

6.8.1 Portée du chiffrement

Tout "paquet" en tant qu'unité de données de protocole (PDU) comporte des informations de commande de protocole (PCI) et des unités de données de service (SDU) au niveau des diverses couches de protocole. Lorsque le chiffrement est appliqué sur le trajet de communication contrôlé, il peut concerner:

- soit la totalité de la pile de protocoles soit une partie de la pile de protocoles (Note 1);
- dans une couche de protocole, soit sur une unité PDU au niveau d'une couche x (Lx) (c'est-à-dire l'unité entière PDU-Lx) soit seulement partiellement (c'est-à-dire les seules parties informations PCI ou l'unité SDU).

NOTE 1 – Exemple: un service en mode paquet RTP sur IP peut assurer le chiffrement:

- a) sur une couche réseau (par exemple, selon le mode transport IPsec ou le mode tunnel IPsec);
- b) sur une couche transport (par exemple, selon le mode DTLS); ou/et
- c) sur une couche application (par exemple, selon le mode SRTP).

Le contrôle DPI peut s'effectuer sur toute partie non chiffrée du paquet.

R-6.8.1/1: Détermination de l'existence d'un trafic chiffré (du point de vue de la signature DPI): le contrôle DPI peut à titre facultatif être effectué sur tous les éléments d'information non chiffrés du trafic contrôlé, en fonction de l'étendue du chiffrement (Note 2).

NOTE 2 – Exemple: un flux de paquets SRTP sur IP peut toujours être contrôlé dans le cas de signatures DPI, sur la base des éléments d'information concernant les commandes de protocole PCI RTP ("en-tête RTP"), PCI UDP ("en-tête UDP"), PCI IP ("en-tête IP"), etc., si seule l'unité SDU RTP (contenant les données d'application IP) est chiffrée.

R-6.8.1/2: Non-détermination de l'existence d'un trafic chiffré (du point de vue de la signature DPI): le contrôle DPI peut à titre facultatif être effectué partiellement (parce que des parties des signatures DPI peuvent concerner des éléments d'information sur des paquets non chiffrés).

Un tel "contrôle partiel" sur le trafic chiffré peut conduire à des "services de contrôle limités", mais déjà suffisants pour des cas d'utilisation spécifiques (par exemple, lorsqu'une identification "grossière" d'une application ou d'un protocole peut être déjà suffisante).

6.8.2 Disponibilité d'une clé de chiffrement

R-6.8.2/1: Le contrôle DPI peut à titre facultatif être appliqué dans le cas de la disponibilité locale de la ou des clés de chiffrement employées. Toute exécution du contrôle DPI impliquera dès lors le déchiffrement initial (d'une copie à l'échelle locale) du paquet contrôlé.

6.8.3 Conditions relatives aux contrôles fondés sur des informations chiffrées

R-6.8.3/1: Le contrôle DPI peut à titre facultatif être effectué sur un trafic chiffré, lorsqu'il existe des conditions politiques applicables aux contrôles fondés sur des informations chiffrées (Note).

NOTE – Exemple: une configuration binaire (qui identifie sans ambiguïté un flux de paquets particulier) peut être déduite de l'observation (du contrôle) d'un trafic partiellement chiffré (voir le § 6.8.1). La configuration binaire, en tant que partie des signatures DPI suivantes, serait alors déjà disponible dans le codage chiffré.

6.8.4 Spécifications relatives au contrôle DPI dans le cas du protocole IPsec

Les spécifications énoncées dans les § 6.8.1 à 6.8.4 valent aussi pour les paquets chiffrés IPsec. La présente Recommandation vise les aspects concernant l'identification des flux du trafic chiffré IPsec. Les aspects concernant l'identification de l'application doivent faire l'objet d'un complément d'étude.

6.8.4.1 Spécifications générales

R-6.8.4.1/1: L'entité DPI-FE peut à titre facultatif être en mesure d'assurer au moins l'identification du flux pour le trafic chiffré IPsec. Le n-uplet correspondant du descripteur de flux peut à titre facultatif être limité aux seuls éléments des couches L2 et L3.

R-6.8.4.1/2: Un flux peut à titre facultatif correspondre au trafic d'une seule association de sécurité IPsec ou peut à titre facultatif concerner de multiples associations.

R-6.8.4.1/3: L'identification du flux fondé sur l'association de sécurité implique que l'indice du paramètre de sécurité IPsec (SPI) à 32 bits peut à titre facultatif faire partie du descripteur de flux.

6.8.4.2 Mode tunnel IPsec et mode transport IPsec

Les protocoles IPsec (concernant l'en-tête d'authentification (AH) et les données utiles pour la sécurité d'encapsulation (ESP)) peuvent être utilisés pour protéger, soit la totalité des données utiles IP (en mode tunnel), soit les données utiles IP des protocoles de couche supérieure (en mode transport).

R-6.8.4.2/1: L'entité DPI-FE peut à titre facultatif être en mesure de détecter le trafic chiffré IPsec en mode tunnel.

R-6.8.4.2/2: L'entité DPI-FE peut à titre facultatif être en mesure de détecter le trafic chiffré IPsec en mode transport.

6.8.4.3 Trafic IPsec protégé par l'en-tête d'authentification

L'en-tête d'authentification (AH) assure l'intégrité des données, l'authentification de l'origine des données et fournit à titre facultatif des services limités contre la réexécution.

R-6.8.4.3/1: L'entité DPI-FE peut à titre facultatif être en mesure de détecter un trafic protégé par l'en-tête d'authentification en se fondant sur le numéro du protocole IP correspondant.

6.8.4.4 Trafic IPsec protégé par les données utiles pour la sécurité d'encapsulation

Les données utiles pour la sécurité d'encapsulation (ESP) assurent en outre la confidentialité.

R-6.8.4.4/1: L'entité DPI-FE peut à titre facultatif être en mesure de détecter un trafic protégé par les données ESP en se fondant sur le numéro du protocole IP correspondant.

6.9 Contrôle du trafic comprimé

La compression a pour objet de réduire le volume du trafic. Par exemple:

- la compression "ZIP" [b-IETF RFC 1950] réduit la taille des fichiers (applicable aux flux FTP sur TCP/IP);
- la compression "SigComp" [b-IETF RFC 3320] réduit la taille des messages SIP (applicable aux flux SIP sur L4/IP).

6.9.1 Détermination de la méthode de compression

R-6.9.1/1: Le contrôle DPI peut à titre facultatif être effectué lorsque des informations sur la méthode de compression appliquée sont disponibles localement (c'est-à-dire lorsque le nœud DPI est informé du fait que le trajet de signalisation SIP est codé conformément au § 8 de la référence [b-ETSI TS 124 229]). Tout contrôle DPI pourrait alors conduire à une décompression initiale (de la copie locale) du paquet contrôlé.

R-6.9.1/2: Le contrôle DPI peut à titre facultatif être effectué lorsque le flux de trafic contrôlé permet de déterminer la méthode de compression appliquée (par exemple, la méthode de compression zip particulière peut à titre facultatif être déterminée à partir des éléments d'information de l'en-tête de fichier).

6.10 Détection d'un trafic anormal

6.10.1 Spécifications relatives à la détection d'un trafic anormal

R-6.10.1/1: L'entité DPI-FE doit être en mesure d'assurer la détection d'un trafic anormal. Notamment, les signatures doivent pouvoir caractériser un trafic normal ou anormal (par exemple, comme faisant partie d'une liste noire ou d'une liste blanche).

NOTE – Aspects concernant les règles de politique DPI: Cette capacité peut impliquer la vérification des nombreuses mesures relatives aux caractéristiques du trafic et/ou des paquets, ainsi qu'éventuellement l'établissement d'une arborescence de décisions pour la conclusion finale concernant les classes de trafic normal ou anormal.

7 Spécifications fonctionnelles du point de vue du réseau

7.1 Spécifications générales

7.1.1 Télécommunications d'urgence

Globalement, la conception, la mise en œuvre, le déploiement et l'utilisation des fonctions DPI doivent inclure des mesures appropriées qui permettent d'éviter des effets nuisant à la performance et à la sécurité des télécommunications d'urgence (ET). Par télécommunications d'urgence [UIT-T Y.2205], on entend tout service associé à une urgence, qui nécessite un traitement spécial, comparé aux autres services (c'est-à-dire, un traitement prioritaire par rapport aux services réguliers). Sont concernés les services d'urgence agréés par les pouvoirs publics, par exemple les services de télécommunications d'urgence [UIT-T E.107] et les services de sécurité publique.

La présente Recommandation est fondée sur l'emploi d'une étiquette d'application pour identifier de façon générique les différentes sémantiques d'application telles que le type du protocole d'application (par exemple, vidéo UIT-T H.264 ou SIP en tant qu'exemple de protocole d'application IP). Les mêmes types d'application (par exemple, SIP) sont employés pour assurer tant les services réguliers que les services de télécommunications d'urgence. Comme la présente Recommandation ne spécifie pas une étiquette d'application unique permettant d'identifier les services de télécommunications d'urgence, il convient de prendre les précautions nécessaires pour éviter que les services de télécommunications d'urgence ne subissent des conséquences néfastes.

R-7.1/1: On ne doit pas interférer avec le traitement prioritaire du trafic des services de télécommunications d'urgence par rapport aux services ordinaires.

R-7.1/2: La conception globale, la mise en œuvre, le déploiement et l'utilisation des fonctions DPI doivent comporter des mesures appropriées qui permettent d'éviter des effets nuisant à la performance des services de télécommunications d'urgence (par exemple, en introduisant des délais inutiles).

R-7.1/3: La conception globale, la mise en œuvre, le déploiement et l'utilisation des fonctions DPI doivent comporter des mesures appropriées qui permettent d'éviter les atteintes en matière de sécurité visant l'intégrité, la confidentialité ou la disponibilité des communications ou des sessions de télécommunication d'urgence

NOTE – La présente Recommandation ne spécifie pas de quelle manière il convient de satisfaire aux spécifications. Celles-ci peuvent être satisfaites en employant des capacités fonctionnelles, des mesures opérationnelles ou les deux.

7.2 Plan de données, plan de commande et plan de gestion dans un nœud DPI

7.2.1 Plans de trafic et types de trafic du point de vue d'un nœud DPI

Selon le modèle de réseau comportant le plan de l'utilisateur, le plan de commande et le plan de gestion (voir la référence [b-UIT-T Y.2011]), un nœud DPI concerne un trajet de données et un trajet de décision locale (voir la Figure 7-1). Le trajet de données peut s'effectuer soit en mode unidirectionnel soit en mode bidirectionnel.

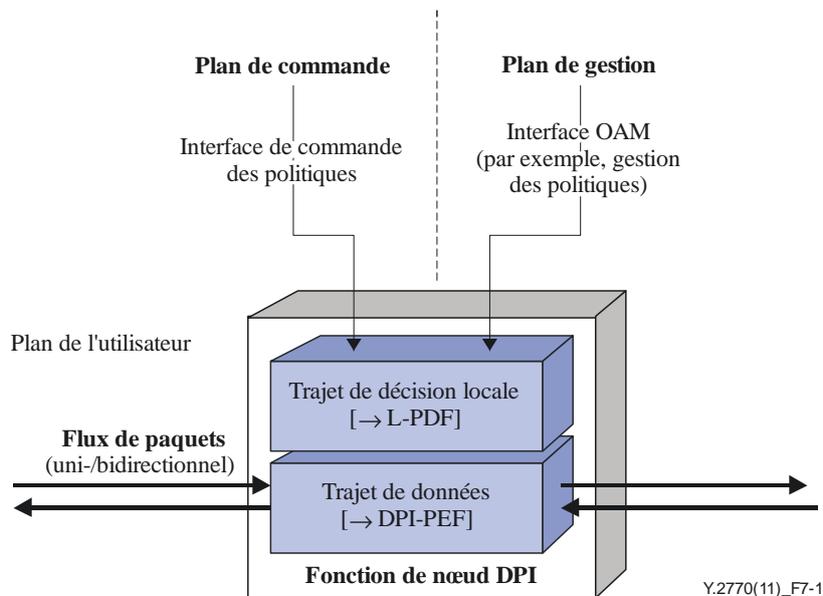


Figure 7-1 – Plans de trafic externe et interne d'un nœud DPI

NOTE 1 – Les flux de paquets sont acheminés/commutés sur des trajets de paquets, souvent nommés trajets de données dans les réseaux IP (voir par exemple la référence [b-IETF RFC 4778]); en raison de cela, le terme plan de données est synonyme du terme plan de l'utilisateur.

NOTE 2 – Le trajet de données IP est aussi connu sous le nom de trajet média IP (ou trajet support) dans le cas du trafic de données d'application IP, ou sous le nom de trajet de signalisation IP dans le cas du trafic de commande d'application IP [b-UIT-T X.1141].

R-7.2.1/1: Un nœud DPI doit prendre en charge l'interface du plan de gestion pour la gestion des politiques et peut à titre facultatif prendre en charge l'interface du plan de commande pour la commande des politiques.

L'entité *trajet de décision locale* assure la commande et les capacités de gestion internes au nœud.

R-7.2.1/2: Un nœud DPI doit reconnaître deux types de paquets (voir la Figure 7-2):

- a) les paquets de données, qui appartiennent aux abonnés et acheminent le trafic des abonnés (nommé "trafic THROUGH" ("trafic passant"), voir la référence [b-IETF opsec]);
- b) les paquets de commande et de gestion, qui appartiennent au fournisseur de réseau et concernent l'exploitation du réseau (nommé "trafic TO" ("trafic vers"), voir la référence [b-IETF opsec]).

Les deux types de paquets traversent un "conduit commun" (ou sont "en bande") ou traversent des canaux différents qui séparent sur le plan logique les données des paquets de commande "hors bande" (voir aussi la référence [b-IETF RFC 4778], § 2.2 pour un exemple du trafic de gestion).

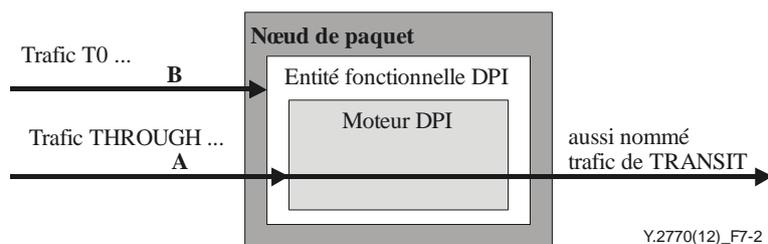


Figure 7-2 – Trafic THROUGH (A) et TO (B) par rapport à un nœud DPI

7.2.2 Spécifications relatives au plan de gestion

R-7.2.2/1: L'entité DPI-FE doit prendre en charge les protocoles de gestion pour la gestion de la configuration des règles de politique DPI.

R-7.2.2/2: Il est recommandé que l'entité DPI-FE assure la gestion des informations concernant l'identité de l'utilisateur et la relation entre l'utilisateur et les applications de l'utilisateur.

R-7.2.2/3: Il est recommandé que l'entité DPI-FE assure la gestion des applications et des services suivants:

- produire, modifier et publier les modèles d'application;
- assurer la relation entre les applications et les stratégies;
- assurer et gérer la réservation des services de l'utilisateur.

R-7.2.2/4: Il est recommandé que l'entité DPI-FE assure la gestion des stratégies prédéfinies ou produites dynamiquement. (Ces stratégies peuvent à titre facultatif concerner l'identification des applications, à la commande des applications et à la gestion de l'utilisateur.)

R-7.1.2/5: Il est recommandé que l'entité DPI-FE assure la gestion de l'autorité d'administration. Pour assurer la gestion hiérarchique, des administrateurs différents ont des autorités de gestion différentes.

7.2.3 Spécifications relatives au plan de commande

R-7.2.3/1: L'entité DPI-FE peut à titre facultatif prendre en charge les protocoles de commande des politiques (tels que dans la référence [b-UIT-T H.248.1] pour le point de référence *Rw* UIT-T défini dans la référence [UIT-T Y.2111]) pour la commande et la signalisation des règles de politique DPI.

7.2.4 Spécifications relatives au plan de l'utilisateur (plan de données)

Le plan de données (plan de l'utilisateur) satisfait aux spécifications facultatives suivantes:

R-7.2.4/1: L'entité DPI-FE peut à titre facultatif prendre en charge les différentes technologies pour les paquets (par exemple, xDSL, UMTS, CDMA2000, câble, LAN, WLAN, Ethernet, MPLS, IP, ATM).

7.2.5 Spécifications applicables à l'ensemble des plans

R-7.2.5/1: L'entité DPI-FE peut à titre facultatif utiliser une grammaire de protocole commune pour la spécification des règles de politique. Il est recommandé que la syntaxe employée au niveau de l'interface de commande des politiques (plan de commande) et de l'interface de gestion des politiques (plan de gestion) soit de préférence la même. Cela n'implique pas l'emploi du même protocole, mais a une incidence sur le langage de spécification pour les règles de politique (DPI) (souvent nommé langage de spécification du filtre (FSL) ou langage de spécification des politiques (PSL); voir la Note).

NOTE – Des langages de script sont, à titre d'exemple, SIEVE [b-IETF RFC 5228] ou PERL ou XML ou XACML (*eXtensible Access Control Markup Language*).

Une grammaire de protocole commune permet d'employer un modèle de données/d'objets commun sur le trajet d'application des politiques dans un nœud DPI, chose prérequis pour une application efficace et rapide des règles ainsi que des opérations de mise à jour sans interruptions dans la bibliothèque des signatures DPI.

8 Interfaces de l'entité fonctionnelle DPI

Les spécifications décrites dans les précédents paragraphes nécessitent les interfaces suivantes:

- entre l'entité DPI-FE et les entités de réseau distantes (voir le § 8.1);
- entre les composants internes de l'entité DPI-FE (voir le § 8.2).

8.1 Interfaces externes de l'entité fonctionnelle DPI

La Figure 8-1 illustre les interfaces externes de l'entité DPI-FE:

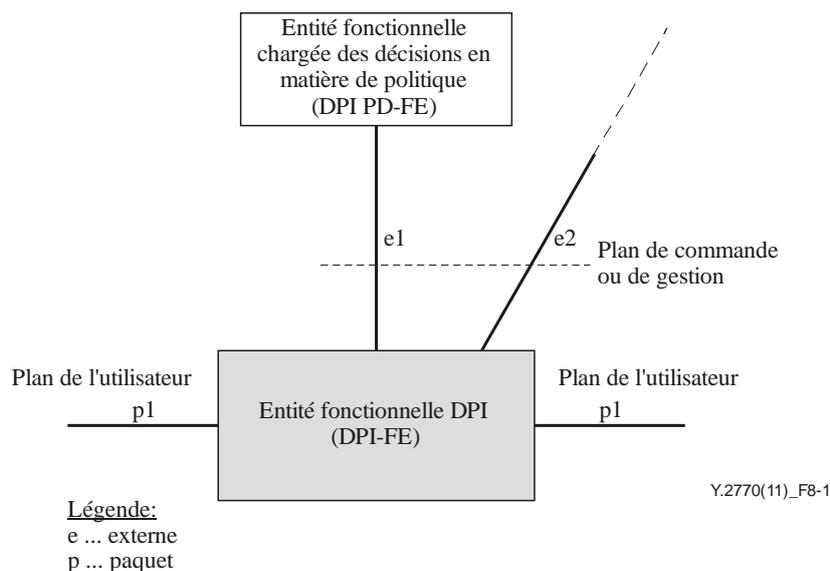


Figure 8-1 – Interfaces externes de l'entité DPI-FE

8.1.1 Trafic contrôlé (p1)

L'entité DPI-FE échange des paquets avec des nœuds de paquets distants par l'interface p1. La topologie du trajet des paquets est une topologie de point à point pour une entité DPI-FE agissant en mode de contrôle DPI sur le trajet. Les topologies multipoint ne sont pas prises en charge. L'interface p1 concerne les trajets de paquets bidirectionnels.

La topologie du trajet des paquets pour une entité DPI-FE agissant en mode de contrôle DPI hors du trajet est associée à l'extrémité.

8.1.2 Commande ou gestion du contrôle du trafic (e1)

L'entité fonctionnelle chargée des décisions en matière de politique (DPI-PDFE) vise à commander ou à gérer l'entité DPI-FE. Les informations échangées par l'interface e1 concernent donc les commandes de contrôle ou de configuration du traitement des paquets par l'entité DPI-FE. Ces commandes peuvent être décrites dans une politique DPI.

L'interface e1 peut aussi assurer la communication de données et la notification par l'entité DPI-FE à l'entité DPI-PDFE.

8.1.3 Communication de données aux autres entités de réseau (e2)

L'interface e2 englobe toutes les interfaces de communication possibles avec les entités de réseau distantes autres que l'entité DPI-PDFE. Cette interface assure essentiellement la communication de données.

8.2 Interfaces internes de l'entité DPI-FE

La Figure 8-2 illustre les interfaces internes possibles sur la base des spécifications relatives au contrôle DPI:

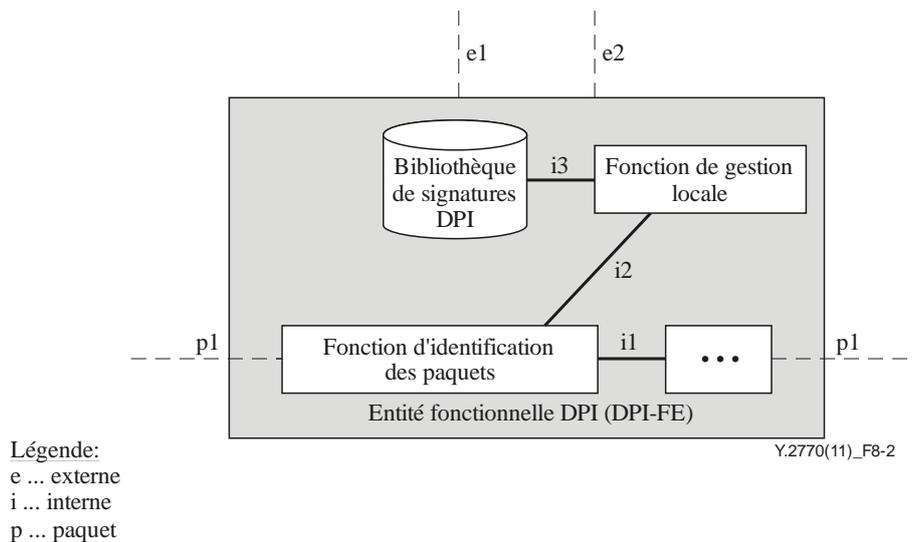


Figure 8-2 – Interfaces internes de l'entité DPI-FE

Il pourrait y avoir d'autres composants fonctionnels internes et interfaces internes de l'entité DPI-FE. Les interfaces internes doivent faire l'objet d'un complément d'étude.

8.3 Spécifications relatives aux interfaces

R-8.3/1: Il est recommandé que l'interface e1 satisfasse aux spécifications du § 6.5.

R-8.3/2: Il est recommandé que l'interface e2 satisfasse aux spécifications du § 6.4.1.

9 Considérations et spécifications en matière de sécurité

Le présent paragraphe décrit les menaces pour la sécurité et définit les spécifications en matière de sécurité pour les entités DPI dans un réseau NGN.

9.1 Menaces pour la sécurité des entités DPI

Les entités fonctionnelles associées au contrôle DPI peuvent d'une façon générale être situées dans une *zone sûre* ou dans une zone sûre mais vulnérable de l'opérateur de réseau NGN, comme défini dans la référence [UIT-T Y.2701]. Cette Recommandation recense les menaces pour la sécurité du réseau NGN et définit les spécifications relatives à la protection contre les menaces. Puisque les entités associées au contrôle DPI font partie du réseau NGN, les conclusions de la référence [UIT-T Y.2701] leur sont applicables. Conformément à la référence [UIT-T Y.2701], les menaces pour la sécurité concernant les entités DPI sont les suivantes:

- destruction des informations concernant le contrôle DPI
- corruption ou modification des informations concernant le contrôle DPI
- vol, suppression ou perte des informations concernant le contrôle DPI
- divulgation des informations concernant le contrôle DPI
- interruption des services.

Les informations ayant trait aux opérations de contrôle DPI comprennent des règles de politique DPI avec leurs signatures ainsi que des informations sur le flux exporté et sur l'application. La destruction, la corruption ou la modification, le vol, la suppression ou la perte de ces informations peut les rendre inutilisables pour les opérations de contrôle DPI. Dans de nombreux pays, il est recommandé que ces informations soient traitées conformément aux spécifications réglementaires et politiques nationales et elles ne doivent pas être divulguées.

Les attaques par déni de service (DoS) peuvent conduire à une interruption des services. Toute entité recevant des données peut être une cible pour les attaques DoS. Par exemple, un attaquant peut indirectement inonder une entité DPI par un grand volume de trafic, causant la dégradation ou l'interruption des services DPI pour les utilisateurs légitimes.

9.2 Spécifications en matière de sécurité pour les entités DPI

Les principales spécifications en matière de sécurité pour les entités DPI sont les suivantes:

R-9.2/1: Les informations concernant le contrôle DPI résidant dans les entités DPI doivent être protégées.

R-9.2/2: Si les informations sont échangées au-delà de la zone sûre de l'opérateur de réseau NGN, les informations concernant le contrôle DPI doivent être protégées entre les entités DPI et les entités fonctionnelles distantes (par exemple, l'entité DPI PD-FE, le système NMS).

R-9.2/3: Des mécanismes peuvent à titre facultatif être nécessaires pour atténuer les attaques sous la forme d'inondations visant l'entité DPI-FE.

R-9.2/4: Les fabricants, les opérateurs et les fournisseurs de services doivent tenir compte des spécifications réglementaires et des politiques nationales lorsqu'ils appliquent la présente Recommandation.

R-9.2/5: Il est recommandé que les responsables de la mise en œuvre emploient les mécanismes existants ayant fait leurs preuves pour satisfaire aux spécifications en matière de sécurité de la présente Recommandation, par exemple, ceux qui sont spécifiés dans la référence [UIT-T Y.2704].

Annexe A

Spécification d'un descripteur de flux

(La présente annexe fait partie intégrante de la présente Recommandation.)

A.1 Point de vue syntaxique du protocole

Le descripteur de flux concerne une structure des données (objet données) qui peut être modélisée comme un k-uplet (voir la Figure A-1). La structure des données consiste en k éléments d'information (IE) (Note). La valeur de k est variable et supérieure à zéro¹, mais constante pour un flux donné. Les éléments d'information sont ceux qui figurent au registre IPFIX de l'autorité IANA. Une valeur est associée à chaque élément d'information. Cette association est généralement une égalité mathématique ('='), Mais d'autres relations mathématiques ne sont pas exclues.

NOTE – Les éléments d'information IPFIX de l'IETF peuvent être attribués comme "champ clé" ou "champ non-clé".

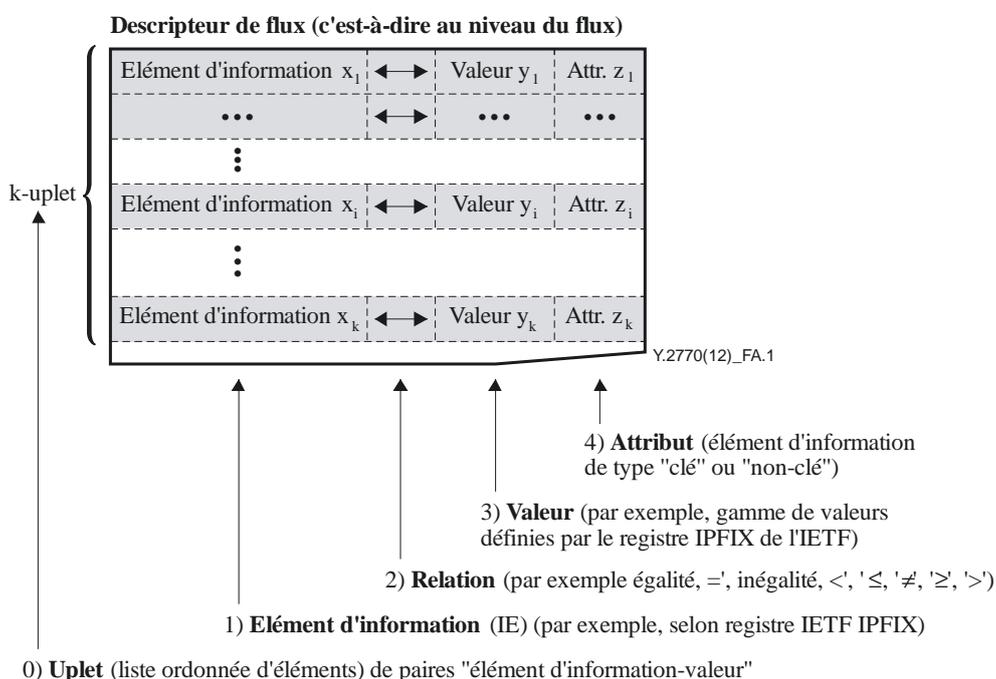


Figure A.1 – Le descripteur de flux (conditions au niveau du flux) du point de vue syntaxique du protocole

Le descripteur de flux comme k-uplet correspond en conséquence à une liste de k "paires nom-valeur" (NVP); ici une suite de paires "< élément d'information ↔ valeur >"².

¹ Note: N = 0 indique "indépendant du flux".

² Semblable à d'autres structures telles que la paire AVP (<nom d'attribut, valeur>), paire paramètre-valeur (<para=valeur>), etc.

A.2 Spécification des valeurs des éléments d'information

Dans les conditions au niveau du flux, la valeur de tout élément d'information peut:

- être complètement spécifiée
La *spécification complète* correspond au cas de la fixation complète des paires nom-valeur;
- non spécifiée
"*Non spécifié*" correspond au cas où *aucune valeur* n'est *encore* attribuée à un élément d'information;
- surspécifiée
La *surspécification* indique que de multiples valeurs sont possibles pour un élément d'information;
- sous-spécifiée
La *sous-spécification* indique des valeurs génériques (par exemple, toutes les valeurs possibles ou des valeurs au choix).

A.3 Relation entre un descripteur de flux, un identificateur de flux IPFIX et une clé de flux IPFIX

L'exemple de la Figure A.2 contient un descripteur quintuplet et 5 clés de flux IPFIX. Afin d'identifier un flux particulier, le descripteur de flux impose certaines conditions sur les valeurs de ces clés de flux telles qu'elles sont définies dans le § A.2: le premier élément d'information de la clé de flux x1 est "complètement spécifié", le deuxième élément d'information x2 est "surspécifié", tandis que les autres ne sont "pas spécifiés", comme illustré dans la partie a) de la Figure A.2.

a) ... Des conditions au niveau du flux, qui peuvent partiellement correspondre aux informations sur la clé de flux IPFIX, sont fournies à l'entité DPI-FE ...

Descripteur de flux

IE x_1	=	Complètement spécifié y_1	"Clé"
IE x_2	>	Surspécifié y_2	"Clé"
IE x_3		Non spécifié	"Clé"
IE x_4		Non spécifié	"Clé"
IE x_5		Non spécifié	"Clé"

5 clés de flux IPFIX

b) ... La procédure de contrôle DPI conduit à l'identification de toutes les valeurs observées pour les éléments d'information ...

Identificateur de flux IPFIX (Note)

IE x_1	Valeur observée y_1	"Clé"
IE x_2	Valeur observée y_2	"Clé"
IE x_3	Valeur observée y_3	"Clé"
IE x_4	Valeur observée y_4	"Clé"
IE x_5	Valeur observée y_5	"Clé"

c) ... L'entité DPI-FE peut finalement communiquer des informations sur le flux identifié (par exemple, l'identificateur de flux IPFIX)

Y.2770(12)_FA.2



NOTE – L'identificateur de flux IPFIX est un objet déduit du descripteur de flux, qui n'affecte donc pas le contenu de celui-ci.

Figure A.2 – Exemple de descripteur de flux, d'identificateur de flux IPFIX et de clé de flux IPFIX

Il convient de noter que le descripteur de flux n'impose pas seulement des conditions sur les clés de flux: en effet, dans certains cas, des descripteurs de flux pour des clés autres que des clés de flux peuvent être nécessaires, par exemple lorsqu'une condition pour les fanions TCP du premier paquet est exigée. La différence fondamentale entre le descripteur de flux et l'identificateur de flux IPFIX dans l'exemple de la Figure A.2 est que le descripteur de flux contient une condition "supérieur à" sur l'élément d'information x_2 , ("élément d'information $x_2 > valeur y_2$ "), tandis que l'identificateur de flux IPFIX contient la valeur observée pour l'élément d'information x_2 , à savoir la valeur y_2 . L'identificateur de flux IPFIX est composé de l'ensemble des valeurs observées pour les clés de flux, dès lors que l'entité fonctionnelle a traité les paquets et les a classés en un flux.

Il convient encore de noter que si les informations exportées (par exemple, au moyen d'un enregistrement de flux IPFIX) contiennent chaque élément d'information avec les valeurs observées associées, l'élément d'information étant une clé de flux IPFIX ou non, il n'est pas nécessaire d'attribuer un identificateur de flux IPFIX spécifié, puisque l'identificateur de flux IPFIX est la somme de toutes ces informations.

Bibliographie

- [b-UIT-T H.248.1] Recommandation UIT-T H.248.1 v3 (2005), *Protocole de commande de passerelle: version 3*.
- [b-UIT-T X.734] Recommandation UIT-T X.734 (1992), *Technologies de l'information – Interconnexion des systèmes ouverts – Gestion-systèmes: fonction de gestion des rapports d'événement*
- [b-UIT-T X.1141] Recommandation UIT-T T X.1141 (2006), *Langage de balisage d'assertion de sécurité (SAML 2.0)*.
- [b-UIT-T Y.2011] Recommandation UIT-T Y.2011 (2004), *Principes généraux et modèle de référence général pour les réseaux de prochaine génération*.
- [b-UIT-T Y.2121] Recommandation UIT-T Y.2121 (2008), *Exigences pour la prise en charge d'une technique de transport fondée sur l'état des flux dans les réseaux NGN*.
- [b-ETSI ES 282 003] ETSI ES 282 003 (2011), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture*.
- [b-ETSI TS 123 203] ETSI TS 123 203 (2011), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Policy and charging control architecture (3GPP TS 23.203 version 10.4.0 Release 10)*.
- [b-ETSI TS 124 229] ETSI TS 124 229 (2009), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229 version 9.4.0 Release 9)*.
- [b-IETF IANA IPFIX] IETF IANA IPFIX (2007), *IP Flow Information Export (IPFIX) Entities*.
<<http://www.iana.org/assignments/ipfix/ipfix.xhtml>>
- [b-IETF opsec] IETF draft-ietf-opsec-filter-caps (2007), *Filtering and Rate Limiting Capabilities for IP Network Infrastructure*.
<<http://tools.ietf.org/html/draft-ietf-opsec-filter-caps-09>>
- [b-IETF RFC 1950] IETF RFC 1950 (1996), *ZLIB Compressed Data Format Specification version 3.3*.
- [b-IETF RFC 3198] IETF RFC 3198 (2001), *Terminology for Policy-Based Management*.
- [b-IETF RFC 3320] IETF RFC 3320 (2003), *Signaling Compression (SigComp)*.
- [b-IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.
- [b-IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol*.
- [b-IETF RFC 3871] IETF RFC 3871 (2004), *Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure*.
- [b-IETF RFC 4268] IETF RFC 4268 (2005), *Entity State MIB*.

- [b-IETF RFC 4778] IETF RFC 4778 (2007), *Operational Security Current Practices in Internet Service Provider Environments*.
- [b-IETF RFC 4867] IETF RFC 4867 (2007), *RTP Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs*.
- [b-IETF RFC 5102] IETF RFC 5102 (2008), *Information Model for IP Flow Information Export*.
- [b-IETF RFC 5103] IETF RFC 5103 (2008), *Bidirectional Flow Export Using IP Flow Information Export (IPFIX)*.
- [b-IETF RFC 5228] IETF RFC 5228 (2008), *Sieve: An Email Filtering Language*.
- [b-IETF RFC 5424] IETF RFC 5424 (2009), *The Syslog Protocol*.
- [b-IETF RFC 5426] IETF RFC 5426 (2009), *Transmission of Syslog Messages over UDP*.
- [b-IETF RFC 5476] IETF RFC 5476 (2009), *Packet Sampling (PSAMP) Protocol Specifications*.
- [b-PacketTypes] McCann, P.J., and Chandra, S. (2000), *PacketTypes: Abstract Specification of Network Protocol Messages*; SIGCOMM '00: Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, pp. 321-333, ACM Press, New York.

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication