Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.2771

(07/2014)

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

Réseaux de prochaine génération – Sécurité

Cadre pour l'inspection approfondie des paquets

Recommandation UIT-T Y.2771

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
Améliorations concernant les réseaux de prochaine génération	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.2771

Cadre pour l'inspection approfondie des paquets

Résumé

La Recommandation UIT-T Y.2771 définit un cadre pour l'inspection approfondie des paquets (DPI, *deep packet inspection*). L'objectif premier de ce cadre est de décrire une approche structurée permettant de concevoir, de définir et de mettre en œuvre des solutions DPI à l'appui de la prise en compte des services/applications pour faciliter l'interopérabilité dans les réseaux en évolution. Cette Recommandation permet d'identifier les aspects relatifs aux réseaux et d'en faciliter la compréhension, principalement du point de vue de l'architecture. Elle traite en outre d'aspects relatifs au cadre DPI du point de vue de la modélisation et de la performance.

De tels cadres visent en particulier à décrire les relations qui peuvent exister entre une fonction DPI et d'autres fonctions de réseau, à faciliter l'identification des exigences relatives aux fonctions DPI (qui font elles-mêmes l'objet d'autres Recommandations UIT-T comme la Recommandation UIT-T Y.2770) et à faciliter les travaux de terminologie (par exemple en cas de relation entre une définition et un modèle fonctionnel).

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T Y.2771	2014-07-18	13	11.1002/1000/12178

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

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/.

TABLE DES MATIÈRES

Recommandation UIT-T Y.2771

Cadre pour l'inspection approfondie des paquets

1 Domaine d'application

La présente Recommandation définit un cadre pour l'inspection approfondie des paquets (DPI) dans les réseaux en mode paquet. Son objectif premier est de décrire les concepts fondamentaux, les composantes fonctionnelles et les capacités applicables à l'inspection DPI à utiliser pour identifier les flux d'information dans les réseaux en mode paquet par le biais des entités DPI, faciliter la spécification d'exigences DPI et aider à élaborer des solutions structurées pour les réseaux en mode paquet (comme les réseaux NGN).

La présente Recommandation donne des informations de haut niveau sur les concepts fondamentaux qui sont généralement applicables pour la réalisation d'entités DPI. Son but n'est toutefois pas de présenter toutes les spécifications détaillées relatives à l'inspection DPI, mais de donner des informations de haut niveau (à savoir un cadre) et de servir de document de base à utiliser par les Commissions d'études de l'UIT et d'autres groupes d'experts extérieurs à l'UIT, par exemple pour l'élaboration de normes détaillées concernant les fonctionnalités DPI.

La présente Recommandation porte sur:

a) les principes architecturaux de base applicables lors de l'intégration de l'inspection DPI dans diverses architectures de réseau;

b) les aspects architecturaux liés aux protocoles du point de vue de l'inspection DPI;

c) des exemples de modèles fonctionnels et de leur application à des cas d'utilisation de l'inspection DPI; et

d) des cadres de performance pour faciliter les analyses de performance de l'inspection DPI, par exemple l'identification d'indicateurs fondamentaux de performance relatifs à l'inspection DPI.

Les responsables chargés de la mise en œuvre et les utilisateurs de la présente Recommandation UIT-T 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 fournisseurs de télécommunication, ainsi que les dispositions de la Constitution et de la Convention de l'UIT.

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.800] Recommandation UIT-T E.800 (2008), *Définitions des termes relatifs à la qualité de service*.

[UIT-T G.602] Recommandation UIT-T G.602 (1988), *Fiabilité et disponibilité des systèmes de transmission analogique en câble et des équipements qui leur sont associés*.

[UIT-T H.248.86] Recommandation UIT-T H.248.86 (2014), *Protocole de commande de passerelle: Prise en charge par les systèmes UIT-T H.248 de l'inspection approfondie des paquets*.

[UIT-T X.200] Recommandation UIT-T X.200 (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), *Technologies de l'information – Interconnexion des systèmes ouverts – Gestion-systèmes: fonction de gestion d'états*.

[UIT-T Y.2704] Recommandation UIT-T Y.2704 (2010), *Mécanismes et procédures de sécurité applicables aux réseaux de prochaine génération*.

[UIT-T Y.2770] Recommandation UIT-T Y.2770 (2012), *Exigences relatives à l'inspection approfondie des paquets dans les réseaux de prochaine génération*.

[ETSI TS 132 410] ETSI TS 132 410 (2012), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Key Performance Indicators (KPI) for UMTS and GSM (3GPP TS 32.410 version 11.0.0 Release 11*.

[IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol – DARPA Internet Program Protocol Specification*.

[IETF RFC 2460] IETF RFC 2460 (1998), *Internet Protocol, Version 6 (IPv6) Specification*.

[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 utilise les termes suivants définis ailleurs:

3.1.1 application [UIT-T Y.2770]: 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)).
- 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 imbriquée dans une autre application (par exemple un contenu d'application dans un élément du corps d'un message SIP ou HTTP).

Une application est identifiable par un identificateur particulier (par exemple au moyen d'un champ binaire, d'un profil, d'une signature ou d'une expression régulière telle que les "conditions au niveau de l'application", voir aussi le § 3.2.2 de [UIT-T Y.2770]), qui est une caractéristique commune à tous les niveaux d'application énumérés ci-dessus.

3.1.2 disponibilité [UIT-T E.800]: un élément est disponible lorsqu'il est en état d'exécuter la fonction requise à un instant donné ou à un instant quelconque d'un intervalle de temps donné, les ressources externes éventuellement requises étant fournies par hypothèse.

3.1.3 descripteur d'application (aussi appelé conditions au niveau de l'application) [UIT-T Y.2770]: ensemble de conditions de règle qui identifient l'application (conformément au § 3.2.1 de [UIT-T Y.2770]).

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.

3.1.4 inspection approfondie des paquets (DPI, *deep packet inspection*) [UIT-T Y.2770]: analyse, conformément au modèle OSI-BRM [UIT-T X.200] à architecture de protocoles en couches,

- des propriétés des données utiles et/ou des paquets (voir la liste des propriétés possibles au § 3.2.11 de [UIT-T Y.2770]) plus en profondeur que les informations d'en-tête des couches de protocole 2, 3 ou 4 (L2/L3/L4); et
- d'autres propriétés des paquets

afin d'identifier l'application sans ambiguïté.

NOTE – Les informations obtenues par la fonction DPI, de même que 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.

3.1.5 moteur DPI [UIT-T Y.2770]: 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 de [UIT-T Y.2770]).

3.1.6 condition de politique DPI (aussi appelée signature DPI) [UIT-T Y.2770]: représentation de l'état et/ou des éléments prérequis nécessaires qui identifient une application et définissent si des actions d'une règle de politique doivent être exécutées. L'ensemble des conditions de politique 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 de 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) 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 de flux ou conditions au niveau du flux (à titre facultatif):
   a) contenu des paquets (champs d'en-tête);
   b) caractéristiques d'un paquet (par exemple le nombre d'étiquettes MPLS);
   c) 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) contenu des paquets (champs d'en-tête de l'application et 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.

3.1.7 entité fonctionnelle de décision de politique DPI (DPI-PDFE, *policy decision functional entity*) [UIT-T Y.2770]: fonction, éloignée de l'entité 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.

3.1.8 descripteur de flux (aussi appelé conditions au niveau du flux) [UIT-T Y.2770]: ensemble de conditions de règle qui est employé pour identifier un type particulier de flux (conformément au § 3.1.3 de [UIT-T Y.2770]) à partir du trafic inspecté.

NOTE 1 – Cette définition du descripteur de flux étend celle qui est donnée dans la Recommandation [b-UIT-T Y.2121] en lui ajoutant des éléments comme décrit au § 3 de [UIT-T Y.2770].

NOTE 2 – Pour une analyse normative plus détaillée du descripteur de flux tel qu'il est utilisé dans la Recommandation [UIT-T Y.2770], voir l'Annexe A de [UIT-T Y.2770].

3.1.9 fiabilité [UIT-T E.800]: probabilité qu'un élément puisse accomplir une fonction requise dans des conditions fixées et pendant un intervalle de temps donné.

3.2 Termes définis dans la présente Recommandation

Les termes suivants sont définis dans la présente Recommandation:

3.2.1 analyseur DPI: entité présente sur le trajet de traitement DPI (à l'intérieur d'une fonction d'application de politique DPI) qui assure essentiellement des fonctions de comparaison entre les en-têtes et les données utiles de paquets particuliers des flux de paquets présélectionnés. L'analyseur DPI vise avant tout à évaluer les *conditions* de politique DPI sur les paquets entrants *présélectionnés*.

NOTE – L'analyseur DPI peut être situé après un scanner DPI (voir le § 3.2.6). Sa fonctionnalité peut être celle d'un analyseur avec système de détection des intrusions (IDS).

3.2.2 nœud DPI: élément de réseau ou dispositif qui intègre les fonctions relatives à l'inspection DPI. Il s'agit donc d'un terme générique employé pour désigner la réalisation d'une entité physique DPI.

NOTE – Sur le plan fonctionnel, la fonction de nœud DPI (DPI-NF) comporte la fonction d'application de politique DPI (DPI-PEF) et la fonction locale de décision de politique (L-PDF) (facultative); la fonction DPI-NF est donc équivalente sur le plan fonctionnel à l'entité fonctionnelle DPI.

3.2.3 action de politique DPI (action en abrégé): définition de ce qu'il faut faire pour appliquer une règle de politique, lorsque les conditions de la règle sont respectées. Les actions de politique peuvent se traduire par l'exécution d'une ou de plusieurs opérations pour modifier et/ou configurer le trafic de réseau et les ressources de réseau, voir également la référence [b-IETF RFC 3198].

3.2.4 fonction d'application de politique DPI (DPI-PEF, *policy enforcement function*): entité logique qui applique les décisions de politique, fondées sur les règles de politique DPI.

3.2.5 scanner DPI (ou "fonction de balayage DPI"): première entité sur le trajet de traitement DPI (à l'intérieur d'une fonction d'application de politique DPI), qui fournit une présélection (pour l'analyseur DPI, voir le § 3.2.1) en vérifiant *toutes* les *conditions* de politique DPI sur *tous* les paquets entrants.

3.2.6 groupe de redondance "1+N" DPI: ensemble de composantes fonctionnelles DPI (par exemple nœud DPI, DPI-PIB, moteur DPI, etc.) constituant une architecture de redondance "1+N" ($N \geq 1$), fondée sur une seule composante active et N composantes de protection.

NOTE – L'ensemble ci-dessus sert à garantir une fiabilité supplémentaire et à améliorer la disponibilité concernant un nœud DPI ou un réseau déployé avec un ou plusieurs nœuds DPI.

4 Abréviations et acronymes

4.1 Abréviations et acronymes généraux

La présente Recommandation utilise les abréviations et acronymes suivants:

A_{DPI} action de politique DPI (*DPI policy action*)

BRM modèle de référence de base (*basic reference model*)

CAM mémoire adressable par le contenu (*content addressable memory*)

C_{DPI} condition de politique DPI (*DPI policy condition*)

DAI identification approfondie de l'application (*deep application identification*)

DHI inspection approfondie de l'en-tête (*deep header inspection*)

DiffServ service différencié (*differential service*)

DPI inspection approfondie des paquets (*deep packet inspection*)

DPI-AcEF fonction d'exécution d'action DPI (*DPI action execution function*)

DPI-AnF fonction d'analyse DPI (*DPI analyser function*)

DPI-FE entité fonctionnelle DPI (*DPI functional entity*)

DPI_{InP} inspection DPI sur le trajet (*in-path DPI*)

DPI-NF fonction de nœud DPI (*DPI node function*)

DPI_{OoP} inspection DPI hors du trajet (*out-of-path DPI*)

DPI-PDFE entité fonctionnelle de décision de politique DPI (*DPI policy decision functional entity*)

DPI-PE entité physique DPI (*DPI physical entity*)

DPI-PEF fonction d'application de politique DPI (*DPI policy enforcement function*)

DPI-PIB base d'informations de politique DPI (*DPI policy information base*)

DPI-PIF fonction d'identification de paquet DPI (*DPI packet identification function*)

DPI-ScF fonction de balayage DPI (*DPI scan function*)

DNNF fonction de détermination du nœud suivant (*determining next node function*)

FIB base d'informations de transmission (*forwarding information base*)

FTP protocole de transfert de fichiers (*file transfer protocol*)

HTTP protocole de transfert hypertexte (*hypertext transfer protocol*)

HW matériel (*hardware*)

IDS système de détection des intrusions (*intrusion detection system*)

IP protocole Internet (*internet protocol*)

IPFIX exportation d'informations de flux IP (*IP flow information export*)

KPI indicateur fondamental de performance (*key performance indicator*)

KPI_{DPI} indicateurs fondamentaux de performance pour les entités DPI (*key performance indicators for DPI entities*)

L-PDF fonction PDF locale (*local PDF*)

L2VPN réseau privé virtuel de couche 2 (*layer 2 virtual private network*)

L_XHI inspection de l'en-tête dans la couche de protocole X (*header inspection of protocol layer X*)

L_XPI	inspection des données utiles dans la couche de protocole X (*payload inspection of protocol layer X*)
LX	couche (de protocole) X (*(protocol) layer X*)
LX+	couche (de protocole) supérieure à la couche LX (*higher (protocol) layer than LX*)
MIB	base d'informations de gestion (*management information base*)
MPI	inspection moyennement approfondie des paquets (*medium depth packet inspection*)
MPLS	commutation par étiquette multiprotocole (*multi-protocol label switch*)
MTBF	durée moyenne entre deux pannes (*mean time between failures*)
MTTR	durée moyenne de réparation (*mean time to repair*)
NA(P)T	traduction d'adresse réseau (et de port) (*network address (and port) translation*)
NGN	réseau de prochaine génération (*next generation network*)
OSI-BRM	modèle de référence de base pour l'interconnexion des systèmes ouverts (*open system interconnection-basic reference model*)
PDF	fonction de décision de politique (*policy decision function*)
PEP	point d'application de politique (*policy enforcement point*)
PFF	fonction de transmission des paquets (*packet forwarding function*)
PIB	base d'informations de politique (*policy information base*)
QoS	qualité de service (*quality of service*)
RACF	fonction de contrôle des ressources et d'admission (*resource and admission control functions*)
R_{DPI}	règle de politique DPI (*DPI policy rule*)
R-PDF	fonction PDF distante (*remote PDF*) (à savoir la fonction PDF située loin du nœud DPI)
RTSP	protocole de diffusion en continu en temps réel (*real time streaming protocol*)
SDU	unité de données de service (*service data unit*)
SIP	protocole d'ouverture de session (*session initiation protocol*)
SPI	inspection peu approfondie des paquets (*shallow packet inspection*)
S_D-PDF	fonction PDF dépendante de la session (*session-dependent PDF*)
S_I-PDF	fonction DPF indépendante de la session (*session-independent PDF*)
SW	logiciel (*software*)
TCAM	mémoire ternaire adressable par le contenu (*ternary content addressable memory*)
TCP	protocole de commande de transmission (*transmission control protocol*)
TOS	type de service (*type of service*)
VoIP	téléphonie IP (*voice over IP*)
VoLTE	téléphonie utilisant la technologie LTE (évolution à long terme) (*voice over long term evolution*)
VoIMS	téléphonie utilisant le système de média intégré (*voice over integrated media system*)
VoNGN	téléphonie utilisant le réseau de prochaine génération (*voice over next generation network*)
VoP2P	téléphonie utilisant la technologie P2P (pair à pair) (*voice over peer to peer*)

4.2 Symboles mathématiques

La présente Recommandation utilise les symboles suivants (nom, brève description et unité):

ε_{DPI}	taux d'erreurs (DPI)	–
$\varepsilon_{f\text{-}n}$	taux de faux négatifs (DPI)	–
$\varepsilon_{f\text{-}p}$	taux de faux positifs (DPI)	–
$\phi_{P,In}$	débit de traitement des paquets entrants (DPI)	[s^{-1}]
$\phi_{P,Out}$	débit de paquets dans le sens sortant (DPI)	[s^{-1}]
$\phi_{P,Node,Out}$	débit du nœud en mode paquet	–
$\phi_{P,Identified}$	débit des paquets identifiés avec succès	–
$P_{Hit,BloomFilter}$	degré de probabilité estimé	–
Ndb	nombre de règles de politique DPI	–
Sp	taille de paquet	–
N_{DPIeng}	nombre de moteurs DPI	–
τ_{TD}	temps de transfert interne au nœud (nœud DPI)	[ns]
$\underline{\underline{A}}$	ensemble d'actions de règle (de politique DPI)	–
$\underline{\underline{C}}$	ensemble de conditions de règle (de politique DPI)	–
$\underline{\underline{R}}$	ensemble de règles (de politique DPI)	–

5 Conventions

Aucune.

6 Cadre architectural

6.1 Cadre relatif à l'architecture du réseau – Scénarios de réseau de haut niveau

Ce cadre définit les principales conditions régissant le déploiement de l'inspection DPI dans une infrastructure de réseau. Certains scénarios de base pour le cadre DPI peuvent être identifiés sur la base de critères tels que:

- **le niveau d'emplacement dans le réseau** (autrement dit l'emplacement d'une entité DPI dans un domaine de réseau en mode paquet)
  - en périphérie ("**DPI périphérique**"); ou
  - à l'intérieur du réseau ("**DPI centrale**");
  - entre réseaux interconnectés ("**DPI d'interconnexion**");
- les types (de trajet) de paquet dans le réseau (autrement dit les types de paquet inspectés)[1]
  - plan d'utilisateur (ou strate de transport; par exemple trajet de données IP, trajet de média IP, trajet support IP, tunnel, LSR MPLS, pseudo-circuit, etc.), ou
  - plan de commande (ou strate des services; par exemple trajet de signalisation IP), ou
  - plan de gestion, ou
  - combinaisons;

[1] On pourrait préciser la notion de "type de paquet" en faisant référence à un "protocole" ou à une "pile de protocoles" en particulier. Ce niveau de détail n'est toutefois pas requis ici.

- **le niveau d'alignement avec d'autres architectures de réseau** (autrement dit le niveau de couplage d'une entité DPI avec l'architecture du réseau en mode paquet sous-jacent)
  - entité **DPI isolée** (autrement dit l'entité DPI est cachée du point de vue du réseau en mode paquet),

    Exemples:
    - très peu d'entités DPI, situées en certains points dans le réseau (sans l'objectif d'une "couverture complète"; inspection DPI sur le trajet de type sondage),
    - entités DPI hors du trajet;
  - réseau **DPI superposé** (autrement dit il existe une infrastructure de réseau DPI dédiée, superposée au réseau en mode paquet sous-jacent; les deux infrastructures de réseau sont distinctes du point de vue opérationnel),

    Exemples:
    - exemple générique: un réseau d'entités DPI sur le trajet qui partagent, par exemple, les trajets dans le plan d'utilisateur, mais utilisent des interfaces de commande et/ou de gestion distinctes;
    - exemple spécifique: par exemple une fonction DPI dont l'objet est de détecter les intrusions;
  - entité **DPI imbriquée** (autrement dit l'entité fonctionnelle DPI est imbriquée dans un élément de réseau physique avec les autres entités fonctionnelles, s'occupant du traitement des paquets non-DPI; une telle entité physique devrait par exemple offrir une seule interface OAM afin d'avoir un fonctionnement présentant un bon rapport coût-efficacité, ce qui suppose par conséquent un modèle de gestion harmonisé pour toutes les entités fonctionnelles),

  Exemples:
    - exemple générique: une entité DPI avec une base d'informations de gestion qui est alignée sur la base de gestion des autres entités fonctionnelles, non-DPI, du même élément de réseau physique;
    - exemple spécifique: une entité fonctionnelle DPI à l'intérieur de la fonction RACF et une capacité de gestion commune, mais sans qu'aucune interface de commande RACF ne soit partagée;
  - entité **DPI intégrée** (autrement dit une entité DPI "entièrement intégrée" dans le "réseau en mode paquet"),

  Exemples:
    - exemple générique: un modèle de référence de réseau (architecture) défini par une organisation de normalisation qui tient compte des entités DPI;
    - exemple spécifique: la fonction RACF de l'UIT-T étendue par des entités DPI pouvant utiliser les points de référence existants (par exemple "entité DPI commandée au point Rw" ou un point Rw de type UIT-T H.248 étendu par la prise en charge de [UIT-T H.248.86]) ou pouvant créer de nouveaux points de référence;

Il existe donc de nombreux cas d'utilisation en ce qui concerne le scénario d'intégration d'une entité DPI dans le réseau.

6.2 Cadre relatif à l'architecture des protocoles – Niveau d'inspection des paquets pour certains exemples d'applications de réseau

6.2.1 Principe

Il existe différents niveaux d'inspection des paquets. Le Tableau 6-1 donne un aperçu des applications de réseau types avec les différents "niveaux d'inspection des paquets" requis. Le niveau d'inspection des paquets peut être indiqué

1) conformément à un modèle de référence de base (BRM) pour les architectures de protocoles en couches, on utilise ici les colonnes L_xHI et L_yPI); ou
2) au moyen d'"anciens" termes informels (qui sont décrits au § 8.1 de [b-UIT-T Y-Sup.23]), on utilise ici les colonnes inspection peu approfondie des paquets (SPI), inspection moyennement approfondie des paquets (MPI), inspection approfondie des paquets (DHI) et identification approfondie de l'application (DAI).

Voir aussi le § 8 de [b-UIT-T Y-Sup.23] sur l'inspection DPI dans les architectures de protocoles en couches.

6.2.2 Distinction des cas DPI et non-DPI

En ce qui concerne les architectures de protocoles en couches, l'inspection DPI a une portée assez large et couvre même toutes les couches de protocole au-dessus de la couche 1 (voir le § 3.2.5 de [UIT-T Y.2770]). Toutefois, la portée de l'inspection des paquets pourrait être limitée dans le cas d'une application de réseau particulière, par exemple aux couches liaison, réseau et/ou transport.

En règle générale, une telle limitation est/était justifiée par des aspects liés au service, au passé ou à la mise en œuvre, par exemple pour l'élaboration de compromis économiques entre un service DPI réalisable et la technique la plus récente. Ce type d'inspection limitée des paquets est/était aussi appelée inspection peu approfondie des paquets ou inspection moyennement approfondie des paquets (SPI, MPI; voir aussi le § 8.1 de [b-UIT-T Y-Sup.23]).

La distinction grossière entre DPI et non-DPI qui est faite dans la Recommandation [UIT-T Y.2770] est suffisante et elle est également retenue dans la présente Recommandation. Par "DPI", on entend ici simplement l'inspection suivant des règles de politique telle qu'elle est prise en charge dans la présente Recommandation, et par "non-DPI", on entend plutôt l'inspection des paquets existante dans les couches de protocole 2, 3 et/ou 4 (à savoir SPI, MPI).

6.2.3 Exemples

Le Tableau 6-1 énumère des exemples d'applications de réseau et les différents niveaux d'inspection des paquets qui sont généralement utilisés dans ces applications de réseau. Il est à noter que les indications figurant dans le Tableau 6-1 ne sont données qu'à titre d'exemple et ne sont pas nécessairement exhaustives.

Tableau 6-1 – Niveau d'inspection des paquets pour certains exemples d'applications de réseau

Application de réseau (exemple)		Niveau d'inspection des paquets				Commentaires
		"Inspection approfondie des paquets" (DPI)				
		NOTE	"Inspection approfondie de l'en-tête" (DHI)		"Identification approfondie de l'application" (DAI)	
			"Inspection moyennement approfondie des paquets" (MPI)			
			"Inspection peu approfondie des paquets" (SPI)			
		Inspection de l'en-tête L2 (L_2HI)	Inspection de l'en-tête L3,4 ($L_{3,4}$HI)	Inspection de l'en-tête L4+ (L_{4+}HI)	Inspection des données utiles L7 (L_7PI)	
Sécurité:						
1.1	Détection des intrusions dans le réseau	–	**X**	**X**	**X**	Il existe différentes méthodes d'identification: a) détection des anomalies; b détection des utilisations abusives (ici)
1.2	Protection de la sécurité des ressources de réseau (prévention des intrusions dans le réseau, prévention des attaques de sécurité)	–	**X**	**X**	**X**	
1.3	Autres fonctions liées à la sécurité					

Tableau 6-1 – Niveau d'inspection des paquets pour certains exemples d'applications de réseau

Identification:						
2.1	Abonné, utilisateur	–	**X**	–	–	Identifié par …? (par exemple l'adresse réseau)
2.2	Type d'application	–	–	**X**	**X**	Identifié par …? (par exemple le type de protocole dans la couche application)
2.3	Session	–	**X**	–	–	Identifiée par …? (par exemple la connexion IP, la connexion de transport IP). Voir aussi le § 7 de [b-UIT-T Y-Sup.23]
2.4	Protocole de commande d'application (par exemple SIP, RTSP, HTTP, FTP, …)	–	**X** (dépend du port connu)	**X**	**X**	
Caractéristiques des données d'application:						
2.5	Contenu	–	–	**X**	**X**	Par exemple contenu illégal
2.6	Type de média (type de données d'application)	–	–	**X**	**X**	
2.7	Format de média	–	–	**X**	**X**	
Modification (des unités de données de protocole):						
3.1	Modification "contenu": suppression des virus	–	–	–	**X**	
3.2	Modification "en-tête": marquage de qualité de service	–	**X**	**X**	–	
3.3	Modification "en-tête & contenu": "fonction ALG"	–	**X**	**X**	–	Fonction NA(P)T locale dans L3 (& L4) et dans la couche application

Tableau 6-1 – Niveau d'inspection des paquets pour certains exemples d'applications de réseau

Surveillance des paramètres d'utilisation:						
4.1	Accords de niveau de service	–	**X**	**X**	**X**	
4.2	Exemples de contrôle des paramètres de trafic:	–	**X**	**X**	**X**	Dépend du type de paramètre de trafic
	Contrôle du débit d'octets L3 (débit maximal, débit admissible)	–	**X**	–	–	
	Contrôle de la taille d'unité PDU L3 (min, max)	–	**X**	–	–	
	Contrôle de la taille de salve L3	–	**X**	–	–	
	Contrôle de la taille d'unité SDU L7 ("données utiles au niveau application")	–	**X**	**X**	–	
	Contrôle du débit d'octets L7 ("volume au niveau application")	–	**X**	**X**	–	
Prise en charge de la qualité de service:						
5.1	Conformation du trafic	–	**X**	–	–	
	Conformation du débit d'octets L3	–	**X**	–	–	Voir par exemple [b-UIT-T Y.1221] ou [b-UIT-T H.248.53]

Tableau 6-1 – Niveau d'inspection des paquets pour certains exemples d'applications de réseau

Analyse du réseau:						
6.1	Comportement des utilisateurs	–	**X**	**X**	**X**	
6.2	Profils d'utilisation	–	**X**	**X**	**X**	
Mesures de la performance ("Indicateurs fondamentaux de performance" (KPI)):						
7.1	Collecte de mesures à distance	–	**X**	**X**	**X**	
7.2	Génération de mesures locales	–	**X**	**X**	**X**	
Prise en charge de la taxation/facturation:						
8.1	Informations relatives à la durée	–	**X**	–	–	
8.2	Informations relatives au volume de trafic	–	**X**	–	**X**	Volume de trafic lié au débit d'octets IP (L3) et/ou aux données d'application
8.3	Informations relatives à l'événement	–	**X**	**X**	**X**	Dépendent du type d'événement (par exemple un événement peut être associé à un contenu)
Inspection DPI orientée liaison:						
9.1	Applications DPI avec éventuellement des conditions de politique liées à la couche 2	**X**	**X**	**X**	**X**	Voir NOTE
NOTE – Une distinction importante est faite entre l'inspection DPI orientée liaison et l'inspection DPI orientée réseau. L'inspection DPI orientée liaison est limitée à un domaine de réseau L2, tandis que l'inspection DPI orientée réseau est liée aux signatures DPI correspondant aux informations de protocole sur la couche réseau (L3) et les couches supérieures.						

7 Cadre de modélisation

7.1 Modèles fonctionnels

Plusieurs modèles fonctionnels sont présentés, illustrant un trajet de transmission des paquets sans aucune inspection DPI (§ 7.1.2), avec une inspection DPI unidirectionnelle (§ 7.1.3) et avec une inspection DPI bidirectionnelle (§ 7.1.4).

Tous les modèles fonctionnels figurant dans le présent paragraphe sont donnés à titre d'exemple.

7.1.1 Inspection DPI sur le trajet ou inspection DPI hors du trajet

Il existe deux principaux scénarios de déploiement d'une fonction de nœud DPI (DPI-NF), du point de vue du trajet des paquets de bout en bout:

- Inspection DPI sur le trajet (DPI_{InP}): la fonction DPI-NF est située sur le trajet des paquets de bout en bout; la fonction d'application de politique DPI (DPI-PEF) exécute les règles de politique DPI directement sur le trafic des paquets (on parle aussi d'inspection DPI en ligne); ou
- Inspection DPI hors du trajet (DPI_{OoP}): la fonction DPI-NF *n'*est *pas* située sur le trajet des paquets de bout en bout, mais elle est centralisée dans le réseau en mode paquet; la fonction DPI-PEF exécute donc les règles de politique DPI indirectement, par exemple sur des échantillons du trafic des paquets (on parle aussi d'inspection DPI indirecte ou d'inspection DPI hors ligne).

Les deux modes DPI sont différents en ce qui concerne le nœud physique hébergeant la fonction DPI-NF: pour l'inspection DPI_{InP}, il peut s'agir d'un nœud en mode paquet, tandis que pour l'inspection DPI_{OoP}, il s'agira en principe d'un nœud *sans* aucune fonction de transmission des paquets (PFF; voir le paragraphe qui suit).

7.1.2 Transmission des paquets générique

Un nœud en mode paquet dans un réseau en mode paquet peut être représenté (à un haut niveau) par une fonction de transmission des paquets (PFF) conformément à la Figure 7-1. La fonction PFF peut par exemple être une fonction de commutation dans le cas de routeurs à commutation par étiquette (LSR) MPLS ou de commutateurs ou ponts Ethernet[2], ou une fonction de transmission/routage dans le cas de routeurs IPv4 [IETF RFC 791] ou IPv6 [IETF RFC 2460]. La fonction PFF doit, pour chaque paquet entrant, déterminer le nœud suivant (par exemple le saut suivant dans les réseaux IP) pour les communications en monodiffusion.

NOTE 1 – Pour la multidiffusion, elle déterminerait plusieurs nœuds suivants.

Pour ce faire, la fonction de détermination du nœud suivant (DNNF) utilise les informations stockées dans une base de données située au même endroit appelée base d'informations de transmission (FIB), par exemple, la base MIB de la table de transmission IP conformément à la référence [b-IETF RFC 4292] dans le cas des routeurs IPv4 définis dans la référence [b-IETF RFC 1812].

---

[2] NOTE – Le terme "paquet" sera alors synonyme de "trame" (L2).

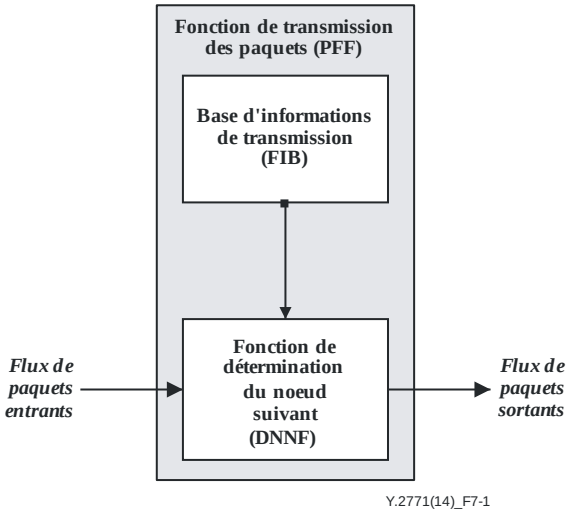


Figure 7-1 – Modèles fonctionnels "transmission des paquets générique"

On notera que la fonction PFF correspond à un modèle unidirectionnel. La fonction DPI (si elle est présente) est située sur le trajet des paquets (à savoir pour le mode DPI sur le trajet (DPI_{InP})), généralement avant la fonction PFF; voir le § 7.1.3.

Les détails et exigences concernant la fonction PFF n'entrent pas dans le cadre de la présente Recommandation; la fonction PFF est toutefois indiquée dans certains modèles fonctionnels afin:

- d'illustrer un comportement de nœud DPI possible sans aucune règle de politique DPI appliquée (par exemple une condition temporaire relative à une base d'informations de politique DPI (DPI-PIB) vide);
- de montrer que des actions de politique particulières, comme "transmettre le paquet", feraient toujours intervenir la fonction PFF; et
- de fournir une spécification de référence non ambiguë pour certains indicateurs de performance liés aux nœuds DPI (voir le § 8).

Il convient de noter que la fonction PFF peut être vide s'il n'y a qu'un seul trajet de paquets (sortant) (NOTE 2).

NOTE 2 – Exemple de scénario: un nœud DPI sur le trajet situé entre deux nœuds en mode paquet L2 ou L3, ou un nœud DPI sur le trajet situé en face d'un équipement d'utilisateur.

7.1.3 Inspection DPI unidirectionnelle

7.1.3.1 Composantes de la fonction d'application de politique DPI unidirectionnelle

7.1.3.1.1 Modèle fonctionnel général de haut niveau

La Figure 7-2 illustre le modèle fonctionnel de haut niveau supérieur, sur la base de l'exemple d'architecture d'une entité fonctionnelle DPI (DPI-FE) donné au § 6.2 de [UIT-T Y.2770].

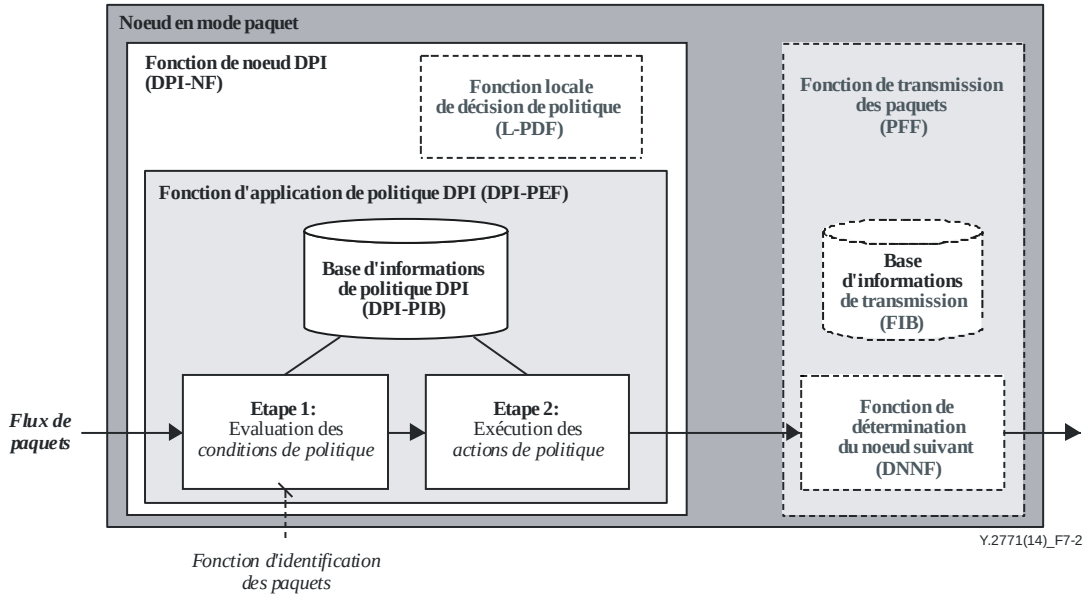


Figure 7-2 – Modèle fonctionnel général de haut niveau

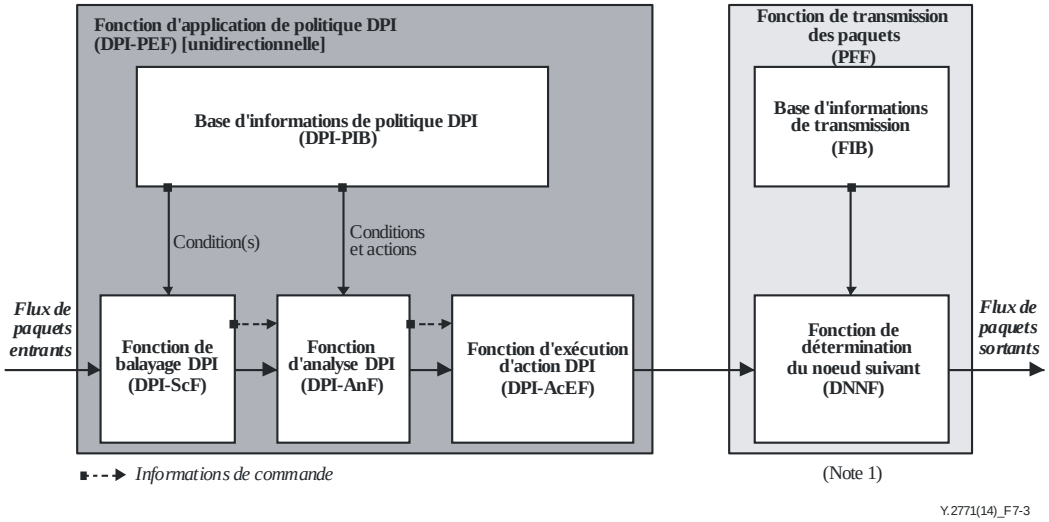
Le trajet des paquets unidirectionnel est modélisé sous la forme d'un processus par étapes. La première étape représente la fonction d'identification des paquets (voir aussi le § 7.3.2.1). C'est une fonction cruciale dans le contexte de l'inspection DPI; elle est décrite plus en détail (par des exemples de modèles de décomposition fonctionnelle) dans les paragraphes qui suivent.

7.1.3.1.2 Composantes de base d'une topologie de traitement en série

La Figure 7-3 illustre un exemple de modèle unidirectionnel (comme modèle possible découlant du modèle de haut niveau de la Figure 7-2). La fonction d'application de politique DPI (DPI-PEF) est située avant la fonction PFF: tout paquet entrant est d'abord traité par la fonction DPI-PEF puis par la fonction PFF. La fonction DPI-PEF peut aussi être structurée en fonctions sur le trajet des paquets auxquelles sont associées une table pour le stockage des règles de politique appliquées, appelée base d'informations de politique DPI (DPI-PIB) ou bibliothèque de signatures DPI. Dans cet exemple, l'application des règles de politique DPI fait intervenir:

- la fonction de balayage DPI (DPI-ScF);
- la fonction d'analyse DPI (DPI-AnF); et
- la fonction d'exécution d'action DPI (DPI-AcEF).

Ces composantes fonctionnelles sont présentées de manière détaillée dans le paragraphe qui suit.



NOTE 1 – La fonction PFF n'entre pas dans le cadre de la présente Recommandation.
NOTE 2 – La fonction PFF n'est présente que pour le mode DPI sur le trajet.

Figure 7-3 – Modèles DPI "composantes de la fonction d'application de politique DPI unidirectionnelle"

7.1.3.1.3 Composantes supplémentaires

7.1.3.1.3.1 A l'intérieur de la fonction DPI-PEF

Les autres composantes de la fonction DPI-PEF ne sont pas encore décrites; elles seront étudiées ultérieurement.

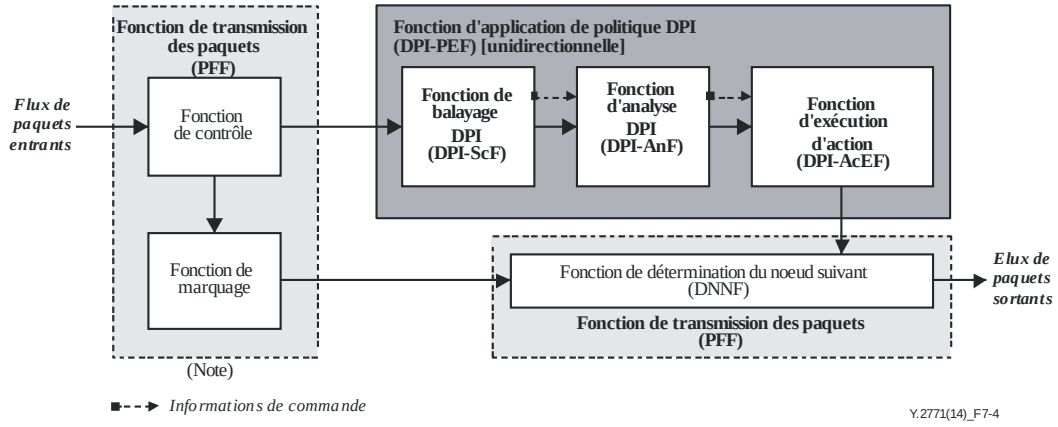
7.1.3.1.3.2 A l'intérieur de la fonction PFF

La fonction de transmission des paquets peut inclure des sous-entités fonctionnelles, par exemple de mise en file d'attente, d'encapsulation, de conformation, de contrôle, de marquage, de commutation, ainsi que la fonction DNNF. Celles-ci n'entrent toutefois pas dans le cadre de la présente Recommandation.

7.1.3.1.4 Aspects structurels du trajet de traitement des paquets

Au lieu d'une exécution en série des fonctions de traitement des paquets (comme illustré dans la Figure 7-3), on pourrait aussi avoir des architectures de nœuds DPI avec des fonctions en parallèle. Par exemple, la fonction PFF pourrait aussi être exécutée parallèlement à la fonction DPI-PEF.

La Figure 7-4 illustre un modèle de trajet avec traitement des paquets en parallèle. Ici, la fonction de contrôle surveille les paquets arrivant à un certain port d'entrée, ou les paquets répondant à des critères prédéfinis (à savoir une condition particulière concernant une règle de politique), par exemple ayant un champ de type de service IPv4 marqué avec une priorité élevée (pour des règles de politique basées sur une inspection SPI). Si ces paquets ou flux entrants transgressent un accord de largeur de bande, la totalité ou une partie des paquets peuvent être marqués en conséquence et envoyés directement à la fonction DNNF.



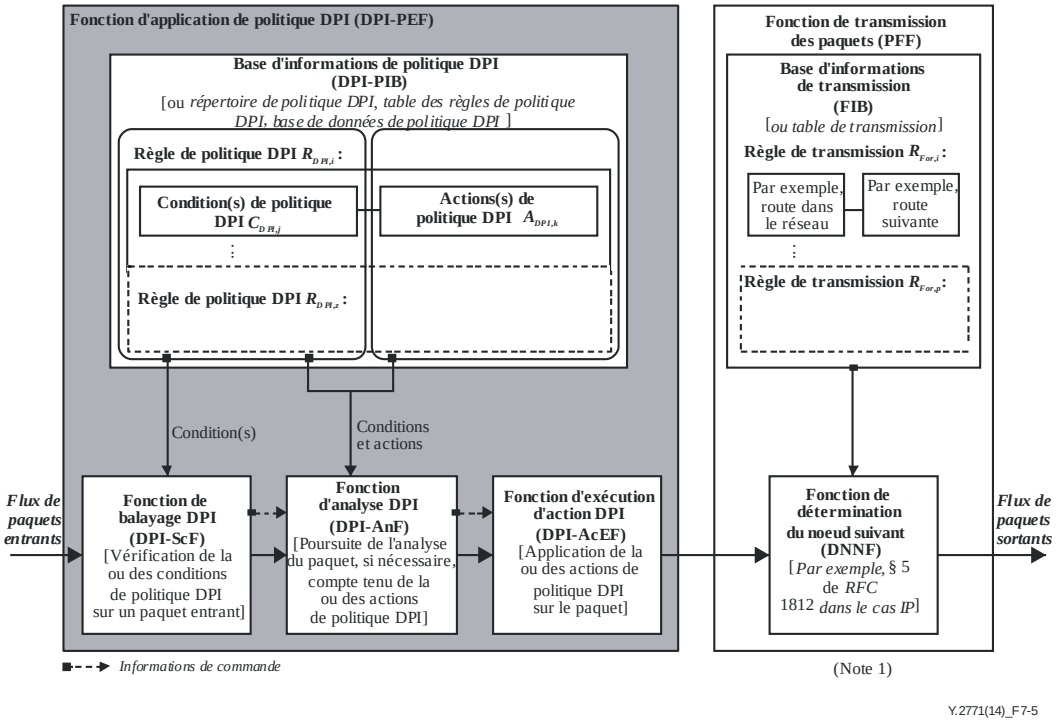
NOTE – La fonction PFF n'entre pas dans le cadre de la présente Recommandation.

Figure 7-4 – Modèle DPI pour la fonction d'application de politique DPI unidirectionnelle avec traitement des paquets en parallèle

Il convient de noter que les exemples des Figures 7-3 et 7-4 représentent des topologies logiques, et non physiques. Dans une mise en œuvre réelle, il convient toutefois de tenir compte du fait que le trajet de traitement des paquets qu'un paquet ou un flux emprunte pourrait être différent, y compris dans une seule instance DPI.

7.1.3.2 Structure de la base d'informations de politique DPI (bibliothèque de signatures DPI)

On trouvera plus de détails sur la base d'informations de politique DPI, en particulier concernant sa structure, dans la Figure 7-5, qui correspond fonctionnellement à la Figure 7-3. La règle de politique (*R*) définit une relation entre un ensemble d'actions (*A*) et un ensemble de conditions (*C*). Les conditions sont évaluées pour déterminer si les actions sont réalisées. En ce qui concerne le terme générique règle de politique, on parle également de règle de filtrage (spécifique) dans le cas d'actions liées aux activités de filtrage des paquets (voir aussi les § 7.3 et 7.6 de [b-UIT-T Y-Sup.23]).



NOTE 1 – La fonction PFF n'entre pas dans le cadre de la présente Recommandation.
NOTE 2 – La fonction PFF n'est présente que pour le mode DPI sur le trajet.

Figure 7-5 – Modèles DPI "Structure de la base d'informations de politique DPI"

Modèle de traitement pour les règles de politique DPI R_{DPI}:

1) La fonction de balayage DPI (DPI-ScF) vérifie toutes (NOTE 1) les conditions de politique DPI C_{DPI} sur un paquet entrant.

   NOTE 1 – Une règle de politique DPI peut couvrir la totalité des paquets transmis par le nœud ou se limiter à un *flux* particulier (voir [UIT-T Y.2770]), donné par un *descripteur de flux* (voir [UIT-T Y.2770]). Le flux de paquets peut par exemple relever d'une *session* de bout en bout (voir le § 6.7 de [UIT-T Y.2770]) entre des instances d'application (par exemple dans le cas d'applications IP, les sessions de bout en bout pourraient être des sessions sur HTTP, RTSP, SIP, FTP, etc. identifiées). L'application de règles de politique propres à la session est souvent appelée contrôle *dépendant de la session*, par opposition au contrôle *indépendant de la session* (auquel cas les règles de politique s'appliquent à la totalité de l'agrégat de trafic d'un nœud d'application de politique). Le présent paragraphe ne donne pas plus de précisions sur le concept de flux et de session, car ce concept n'entre pas en ligne de compte dans les modèles fonctionnels (de haut niveau) représentés.

2) La fonction d'analyse DPI (DPI-AnF) effectue une vérification complémentaire des conditions de politique. Elle intervient après le filtrage initial de chaque paquet par la fonction DPI-ScF (NOTE 2). La fonction DPI-AnF vise à améliorer la performance.

   NOTE 2 – Par exemple, la fonction de balayage peut corréler un paquet entrant avec une application spécifique (par exemple IP), et la fonction d'analyse peut ensuite procéder à une évaluation du paquet en fonction de l'application. La subdivision entre les fonctions DPI-ScF et DPI-AnF repose de manière générale sur un concept d'application de politique en série et/ou de manière hiérarchique (par exemple afin de respecter des objectifs de performance). La fonction DPI-AnF sera étudiée plus en détail ultérieurement.

3) La fonction d'exécution d'action DPI (DPI-AcEF) applique les actions de politique DPI A_{DPI} sur le paquet balayé et analysé.

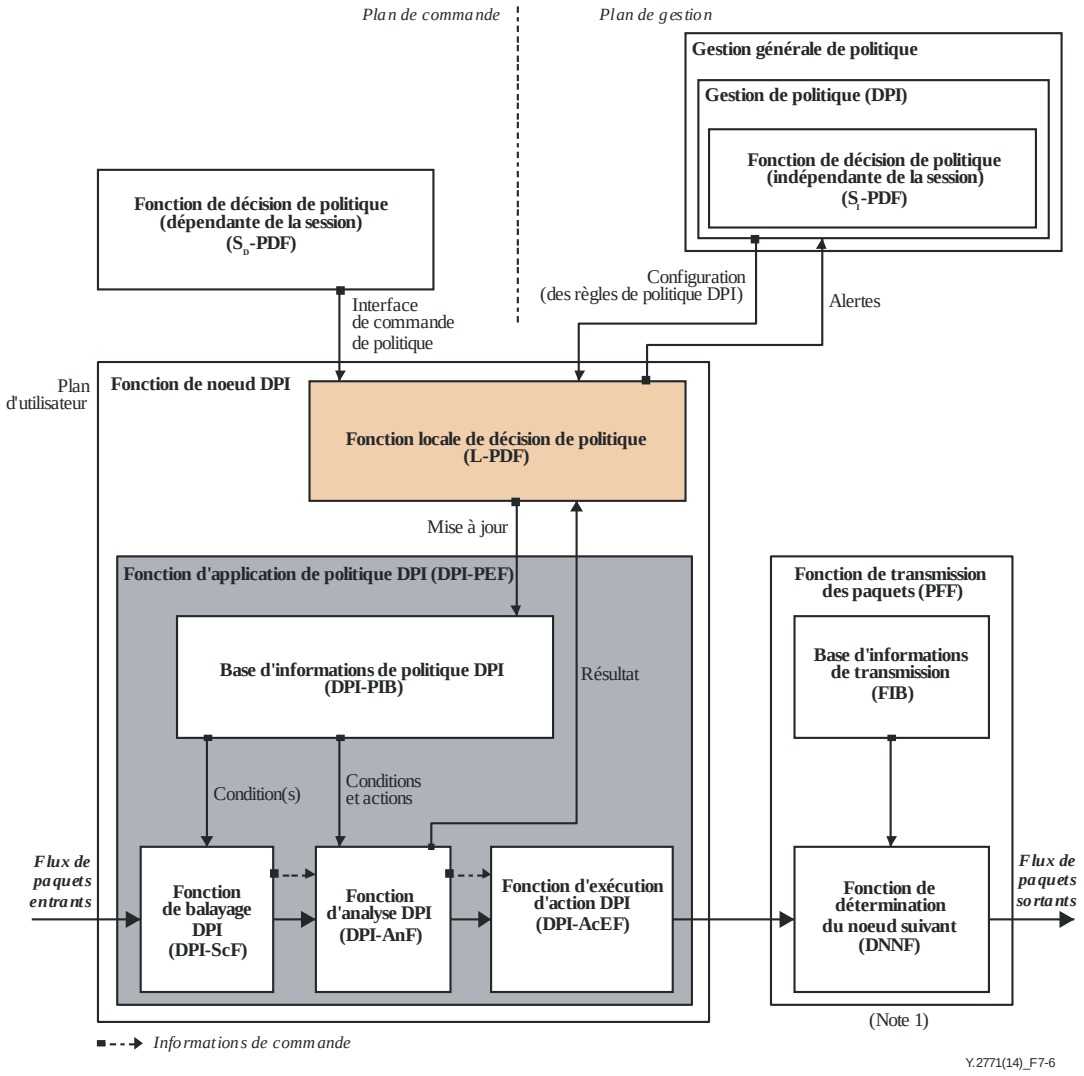
Chaque paquet transmis avec succès par la fonction DPI-PEF sera ensuite traité par la fonction PFF ordinaire (voir aussi le § 7.1.2) dans le cas du mode DPI sur le trajet.

7.1.3.3 Décisions de politique: modification de la base d'informations de politique DPI

La base DPI-PIB contient un ensemble de règles de politique DPI $R_{DPI,i}$, qui déterminent le comportement réel de la fonction DPI-PEF. Les règles de politique DPI sont créées par une entité fonctionnelle de décision de politique (DPI-PDFE). La Figure 7-6 illustre l'exemple de fonctions PDF distantes, situées dans le plan de commande et dans le plan de gestion (la Figure 7-7 décrit un autre exemple de scénario, sans aucun accès (direct) depuis le plan de commande). La fonction PDF du plan de commande peut être chargée des décisions de politique DPI dépendantes de la session (S_D-PDF). Le concept éventuel de session est mentionné dans la Note 1 du § 7.1.3.2. La Recommandation [UIT-T H.248.86] définit une interface de commande de politique. La fonction PDF du plan de gestion peut être chargée des décisions de politique DPI indépendantes de la session (S_I-PDF) (voir la Figure 7-6). La gestion de politique peut avant tout définir des règles de politique dépendantes ou indépendantes de la session (comme dans l'exemple de la Figure 7-7).

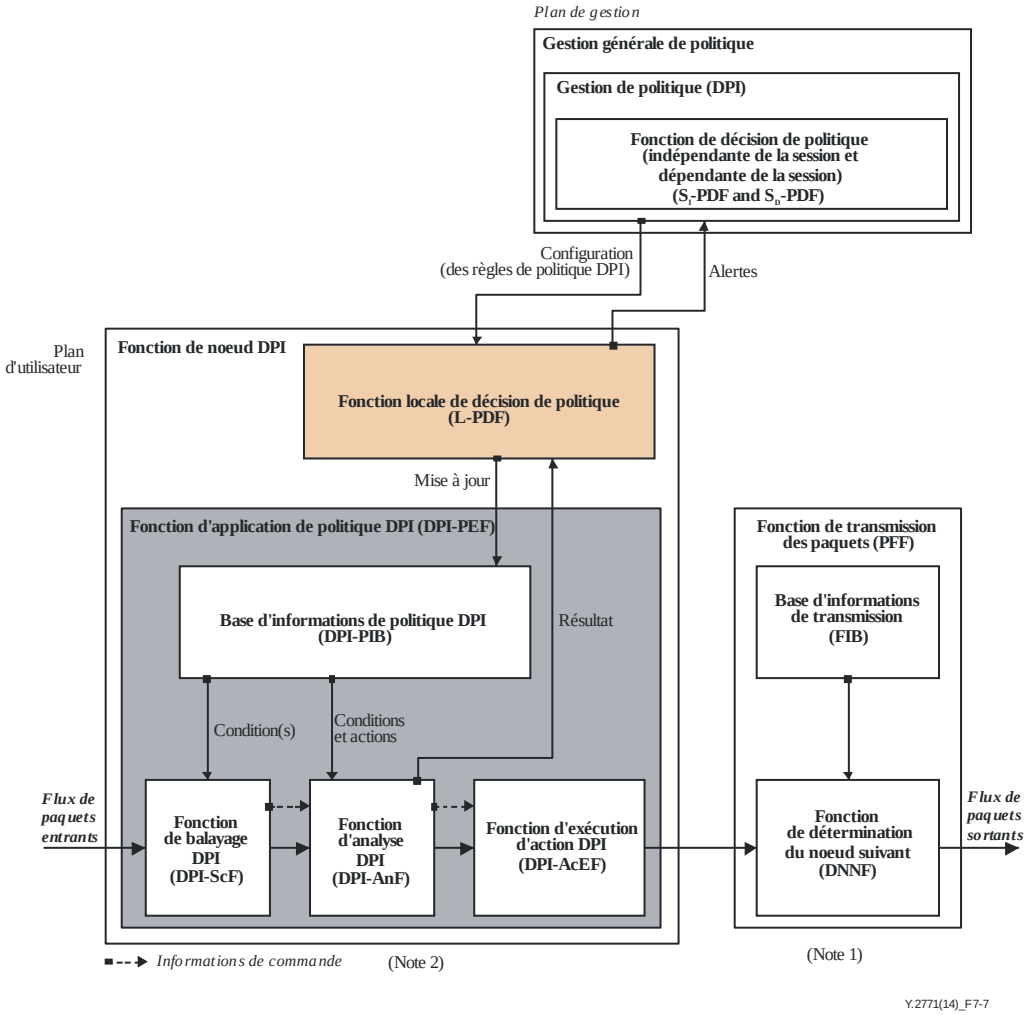
NOTE 1 – Le contrôle dépendant de la session peut par exemple être propre à une application, un utilisateur, un type de média, etc. et le contrôle indépendant de la session peut couvrir des règles de sécurité générales, par exemple des mises à jour quotidiennes. Les règles de politique (DPI) des fonctions S_D-PDF et S_I-PDF sont complémentaires. La Figure 7-4 donne simplement un exemple de configuration du réseau.

En règle générale, la gestion de politique DPI fait partie d'une entité générale de gestion de politique, responsable également des règles de politique non-DPI, concernant par exemple l'inspection des paquets existante – peu approfondie (SPI) ou moyennement approfondie (MPI).



NOTE 1 – La fonction PFF n'entre pas dans le cadre de la présente Recommandation.
NOTE 2 – La fonction PFF n'est présente que pour le mode DPI sur le trajet.

Figure 7-6 – Modèles DPI "Modification de la base d'informations de politique DPI via les plans de commande et de gestion"



NOTE 1 – La fonction PFF n'entre pas dans le cadre de la présente Recommandation.
NOTE 2 – Il se peut que le nœud DPI ne soit connecté à aucun autre élément de réseau du plan de commande.
NOTE 3 – La fonction PFF n'est présente que pour le mode DPI sur le trajet.

Figure 7-7 – Modèles DPI "Modification de la base d'informations de politique DPI via le plan de gestion uniquement"

En règle générale, la ou les fonctions PDF sont situées dans des éléments de réseau distants géographiquement, comme indiqué dans la Figure 7-6 (ainsi que dans la Figure 7-7), rattachés par l'interface de commande de politique pour la fonction S_D-PDF et l'interface de gestion de politique pour la fonction S_I-PDF. Toute fonction PDF distante peut être temporairement hors service, ce qui justifie l'ajout d'une fonction PDF locale (L-PDF) facultative afin d'optimiser la disponibilité du service DPI dans un réseau.

L'ensemble des fonctions L-PDF et DPI-PEF représente la fonction de nœud DPI.

NOTE 2 – La fonction L-PDF correspond au trajet local de décision de politique dans la Figure 7-1 du § 7.2.1 de [UIT-T Y.2770].

La fonction L-PDF (si elle est disponible) assure la communication externe avec la ou les fonctions PDF distantes et l'interface interne avec la fonction DPI-PEF pour la mise à jour de la base DPI-PIB et le traitement des résultats pouvant émaner de la fonction d'analyse DPI (DPI-AnF). La fonction L-PDF peut aussi être chargée de la résolution des éventuels problèmes d'interaction entre les règles de l'ensemble des règles de politique DPI.

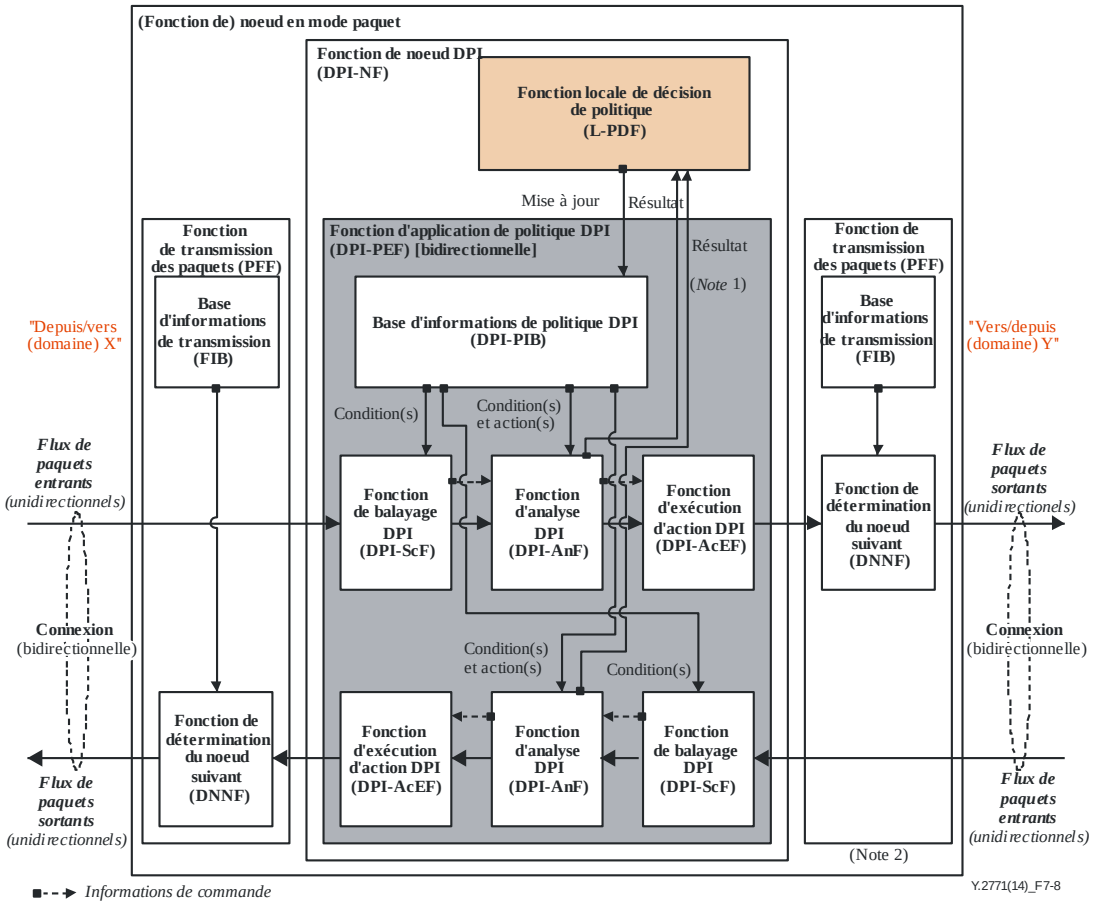
NOTE 3 – La détection et la résolution des interactions entre les règles constituent une fonction fondamentale des fonctions PDF.

Le retour d'information de la fonction d'analyse DPI (DPI-AnF) peut donner lieu à des alertes destinées à la gestion de la politique (par exemple la notification d'une nouvelle menace de sécurité).

Le modèle fondamental d'application de politique est unidirectionnel, mais il peut être étendu afin de prendre en charge des trajets de communication bidirectionnels; voir le paragraphe qui suit.

7.1.4 Inspection DPI bidirectionnelle

La Figure 7-8 montre un exemple de modèle DPI bidirectionnel (pour la définition, voir le § 3.2.4 de [UIT-T Y.2770]). Une connexion en mode paquet bidirectionnelle est constituée de deux flux de paquets unidirectionnels. La base DPI-PIB sert de lien entre les deux sens de trafic du point de vue de l'application de politique DPI. Une règle de politique DPI "bidirectionnelle" définira des conditions et/ou des actions de politique DPI applicables aux deux sens de trafic.



NOTE 1 – La base DPI-PIB peut être organisée en interne en bases DPI-PIB pour chaque sens, par exemple DPIx ® y-PIB et DPIy ® x-PIB.
NOTE 2 – La fonction PFF n'entre pas dans le cadre de la présente Recommandation.
NOTE 3 – Les fonctions PFF ne sont présentes que pour le mode DPI sur le trajet.

Figure 7-8 – Modèles DPI "Inspection DPI bidirectionnelle"

La fonction L-PDF est responsable de la fonction DPI-PEF bidirectionnelle et assure une "fonction de médiation" en procédant au post-traitement des résultats pouvant émaner des fonctions d'analyse (DPI-AnF) unidirectionnelles, ce qui peut ensuite déclencher la mise à jour des règles de politique (locales) et/ou une notification à la ou aux fonctions PDF distantes.

7.1.5 Inspection DPI tenant compte ou non de l'état

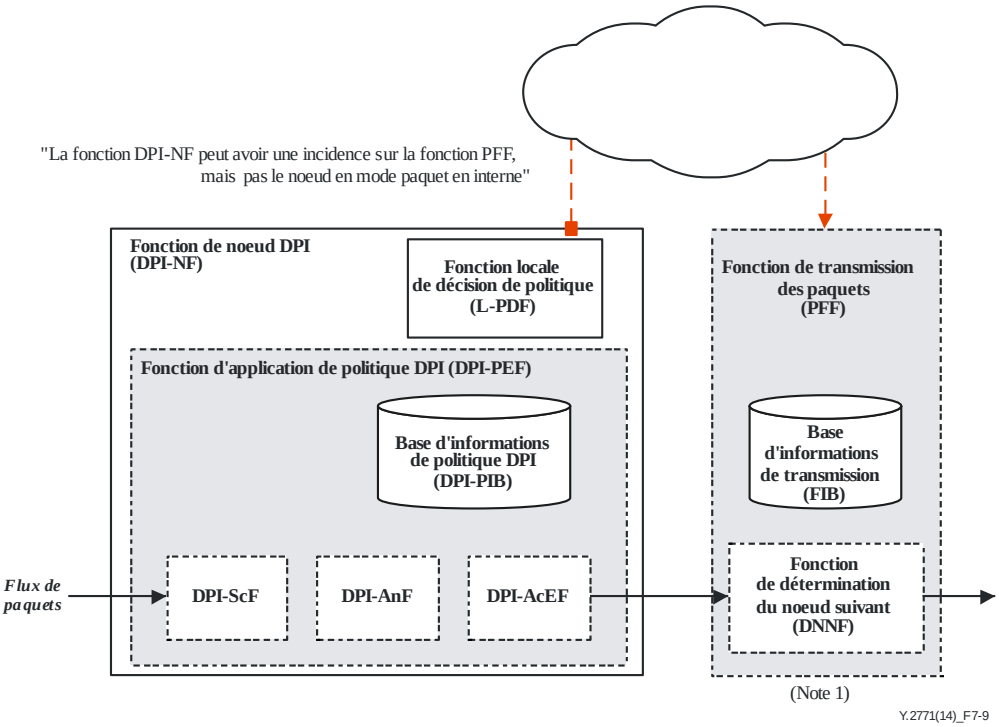
L'inspection DPI ne tenant pas compte de l'état consiste à appliquer les règles de politique DPI à chaque paquet individuellement, sans aucune corrélation avec les autres paquets du flux de paquets unidirectionnel ou de la connexion en mode paquet bidirectionnelle (voir "condition concernant l'état" au § 3.2.11 de [UIT-T Y.2770]).

L'inspection DPI tenant compte de l'état fait intervenir ce type de corrélation (Note), qui peut être modélisée par un automate (fini). Un tel modèle fonctionnel reposera sur des règles de politique DPI concrètes; il n'entre donc pas dans le cadre de la présente Recommandation.

NOTE – Par exemple, une application IP avec transport TCP des données d'application. On pourrait avoir certaines conditions de politique pour la phase d'établissement de connexion TCP et d'autres conditions de politique pour la phase qui suit, à savoir la communication active.

7.1.6 Incidence de l'inspection DPI sur la transmission des paquets

La fonction de nœud DPI peut avoir une incidence sur la fonction de transmission des paquets (PFF) qui suit, à condition qu'une fonction PFF soit disponible et qu'elle ne soit pas vide (voir le § 7.1.2). Toutefois, la fonction DPI-NF ne doit pas être autorisée à apporter des modifications locales à la fonction PFF dans le nœud en mode paquet. Ce type de modifications est en revanche possible à titre d'option, sous la commande d'éléments de réseau distants externes au nœud en mode paquet (voir la Figure 7-9). L'incidence spécifique dépend des décisions de politique et/ou de règles de politique DPI particulières; elle n'entre donc pas dans le cadre de la présente Recommandation.



NOTE 1 – La fonction PFF n'entre pas dans le cadre de la présente Recommandation.
NOTE 2 – La fonction PFF n'est présente que pour le mode DPI sur le trajet.

Figure 7-9 – Incidence possible de l'inspection DPI sur la transmission des paquets via une entité de réseau distante

Exemples:

- Mise à jour de la base FIB (informations sur les routes dans le réseau; voir aussi la Figure 7-5) en fonction de la performance observée dans le réseau en lien avec la topologie du réseau.

- Mise à jour de la base FIB par le blocage de certaines routes dans le réseau (par exemple en sens inverse dans le cas de l'inspection DPI bidirectionnelle).

Il convient de noter que toute modification locale de la fonction PFF, déclenchée par la fonction DPI-NF et commandée par des éléments de réseau externes, doit se faire en lien avec le cadre sous-jacent à l'échelle du réseau en ce qui concerne la transmission, la commutation et/ou le routage des paquets (par exemple domaine DiffServ IPv6, domaine MPLS, topologie L2VPN, etc.).

7.1.7 Inspection DPI à l'intérieur de réseaux en mode paquet et d'environnements NGN

La fonction de nœud DPI est imbriquée dans un nœud en mode paquet fonctionnel, physique ou virtuel, qui peut interagir avec d'autres fonctions dans un réseau en mode paquet. La Figure 7-10 montre un exemple d'environnement. La Recommandation [UIT-T H.248.86] définit une technologie de commande DPI lorsque les entités DPI-PDFE et DPI-FE sont mappées sur un modèle de passerelle décomposée.

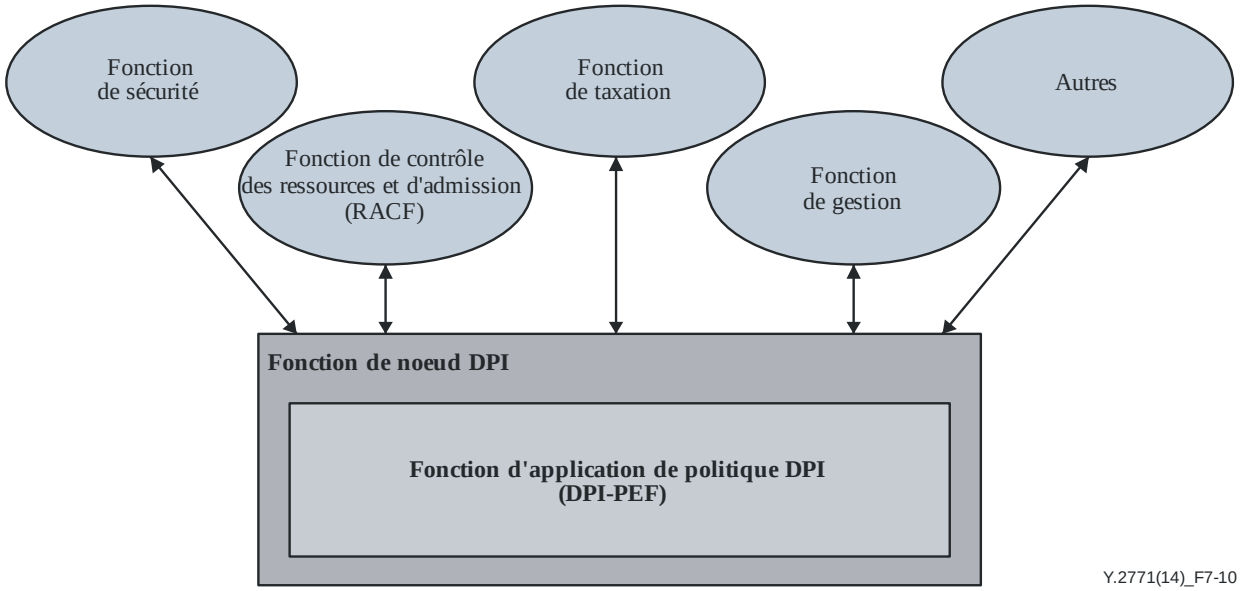


Figure 7-10 – Inspection DPI à l'intérieur de réseaux en mode paquet et d'environnements NGN

7.1.8 Modèles fonctionnels applicables à la prise en charge de la mesure de flux IETF

7.1.8.1 Caractéristique de la fonction de mesure de flux IPFIX IETF

La fonction de mesure de flux IPFIX IETF est définie dans la référence [IETF RFC 5101] (voir aussi le § 6.3.3.2 de [UIT-T Y.2770]). On entend par "flux" un flux de paquets conformément au § 3.1.3 de [UIT-T Y.2770] et par "mesure" la mesure d'indicateurs de performance. La fonction de mesure de flux IPFIX comporte donc une partie avec des *conditions de règle* de politique pour l'identification des flux de paquets (sur la base de l'identificateur de flux IPFIX; voir le § 3.2.17 de [UIT-T Y.2770]) et une partie avec des *actions de règle* de politique pour la réalisation de mesures et la communication des résultats.

7.1.8.2 Fonction de mesure de flux imbriquée

Le processus concernant les flux IPFIX IETF peut être représenté sous forme abstraite et décrit en tant que règle de politique DPI, et par conséquent mappé directement sur une entité DPI-FE. La Figure 7-11 illustre une telle fonction de mesure de flux imbriquée. Les résultats de mesure pourraient être communiqués via les interfaces externes e2 ou e1.

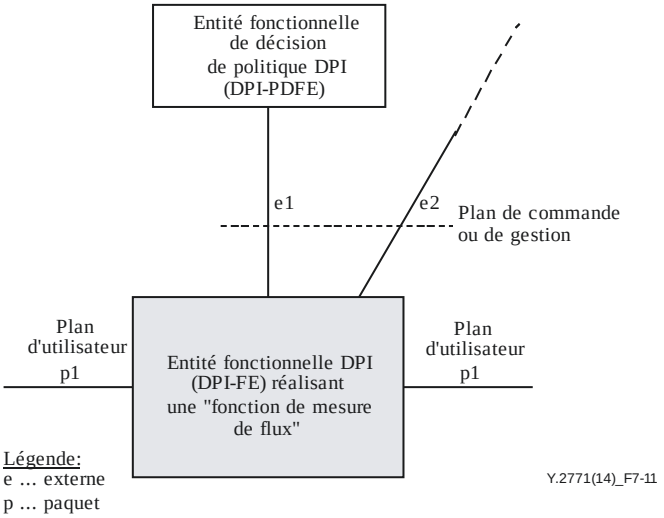


Figure 7-11 – Fonction de mesure de flux imbriquée

7.1.8.3 Fonction de mesure de flux à distance

Une fonction de mesure de flux pourrait aussi être située à distance sur le trajet des paquets p1 – avant (voir la Figure 7-12) ou après une entité DPI-FE. La configuration du réseau avec une fonction de mesure de flux à distance pourrait par exemple se justifier lorsqu'un réseau existant comporte une entité physique prenant en charge la mesure de flux et qu'une entité DPI-FE est de plus déployée.

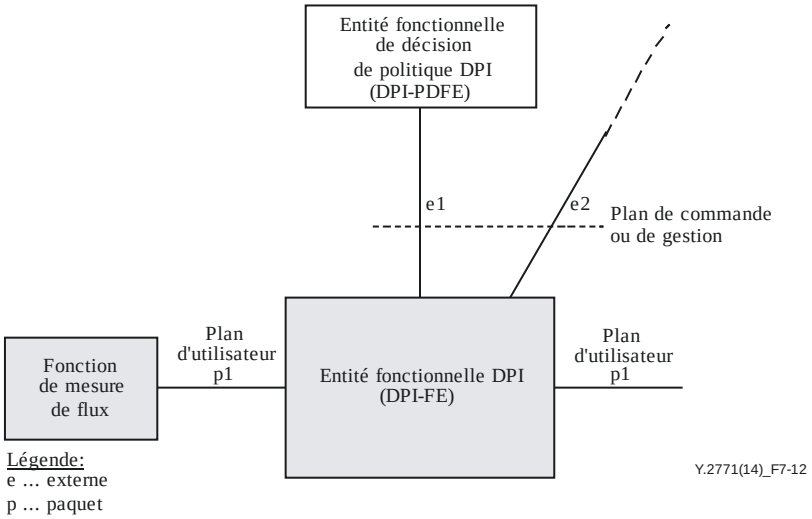


Figure 7-12 – Fonction de mesure de flux à distance

L'entité DPI-FE et la fonction de mesure de flux à distance peuvent être considérées comme une architecture répartie avec deux variantes:

1) Architecture découplée: les deux entités fonctionnelles sont connectées uniquement via p1, et sont donc complètement découplées dans les plans de commande et de gestion.

2) Architecture couplée: à titre d'exemple, les résultats de la fonction de mesure de flux pourraient aussi être communiqués via l'interface e2 de l'entité DPI-FE. Dans un tel modèle de partage fonctionnel, il faudrait ajouter une nouvelle interface (en plus de p1) entre les deux entités fonctionnelles.

Les cas d'utilisation pour les deux variantes seront étudiés ultérieurement.

7.1.9 Inspection DPI probabiliste

7.1.9.1 Inspection DPI probabiliste en général

Le processus d'identification des paquets peut être intrinsèquement de nature statistique (par opposition à l'identification déterministe des paquets), autrement dit, le résultat de l'identification (par exemple selon un critère de concordance) est associé à une probabilité. Ce type d'inspection des paquets est appelé inspection DPI probabiliste, ou inspection DPI incertaine.

Pour l'inspection DPI probabiliste, on utilise des règles de politique DPI dont les conditions sont par exemple:

– Un ensemble de signatures 'S' contenant les signatures 'S_1', 'S_2', …, 'S_N'. Cet ensemble représente une combinaison de conditions de politique suivant une forme normale disjonctive (DNF) booléenne, autrement dit les signatures 'S_i' (i = 1, 2 ... N) sont combinées sous la forme d'une liste de type OU. Les deux étapes de l'inspection DPI sont caractérisées comme suit: étape 1, la génération des conditions de politique est basée sur un processus probabiliste; et étape 2, l'exécution des conditions de politique conduit à des résultats de concordance déterministes, ce qui conduit globalement à une inspection DPI probabiliste.

L'objectif premier de l'inspection DPI probabiliste est de déterminer rapidement et efficacement si un paquet concorde avec l'ensemble de signatures 'S'. L'information concrète de concordance – à savoir la signature spécifique 'S_i' qui a été identifiée – est secondaire. L'ensemble de signatures 'S' représente en général une option d'identification pour une application donnée. L'étiquette d'application associée, par exemple 'Paquet avec signature dans l'ensemble S', pourrait être communiquée.

7.1.9.2 Inspection DPI probabiliste basée sur un filtre de Bloom

Une inspection DPI basée sur un filtre de Bloom est un exemple bien connu d'inspection DPI probabiliste, en raison du taux d'erreurs intrinsèque ε_{DPI} – en termes de faux positifs $\varepsilon_{f\text{-}p}$ (voir le § 8.2.3.3.1) – de l'approche sous-jacente d'inspection des paquets.

Considérons un exemple d'utilisation d'un filtre de Bloom pour une application donnée:

– L'application DPI est la détection du "trafic de l'application x". Le trafic de l'application x est caractérisé par l'ensemble de signatures S = {'application x v1', 'application x v2', …, 'application x vk'}, autrement dit les différentes signatures concernant les caractéristiques propres à l'application. On pourrait alors par exemple utiliser, pour détecter si un paquet correspond à l'"application x", une règle de politique DPI reposant sur l'ensemble de signatures ci-dessus en tant que combinaison de conditions de règle de politique DPI, et simplement éliminer le paquet en cas de concordance sans qu'il soit nécessaire de connaître la version exacte de l'application x.

  Le principal atout de l'inspection DPI probabiliste basée sur un filtre de Bloom tient à la possibilité de choisir un compromis entre la précision de l'identification et la consommation de ressources d'identification (par exemple en termes d'utilisation du processeur et/ou de la mémoire). Une telle approche permet de simplifier considérablement le traitement DPI.

Le caractère probabiliste de l'inspection DPI basée sur un filtre de Bloom est donné par le processus suivant:

– Tout paquet arrivant 'P' est comparé au filtre de Bloom représentant la totalité de l'ensemble de signatures 'S' en parallèle; si un paquet 'P' concorde avec une ou plusieurs signatures de l'ensemble 'S', le résultat est une concordance avec un degré de probabilité estimé à $P_{Hit,BloomFilter,'S'}$, donné par:

$$P_{Hit,BloomFilter,'S'} = 1 - \varepsilon_{f-p} = 1 - \left(1 - e^{-kN/m}\right)^k \qquad (7\text{-}1)$$

les paramètres étant les suivants:

m = taille du filtre de Bloom en bits

N = nombre de signatures dans l'ensemble S

k = nombre de fonctions de hachage utilisées pour la création du filtre de Bloom.

Le qualificatif "probabiliste" renvoie à la "précision d'identification" d'un paquet, d'un flux, d'une application, etc. par l'entité DPI-FE, cette précision étant étroitement liée aux indicateurs de performance en termes de taux d'erreurs (voir le § 8.2). En ce qui concerne l'inspection DPI probabiliste réalisée par des filtres de Bloom, voir l'Appendice I, avec l'indicateur de performance "taux de faux positifs (DPI)" $\varepsilon_{f\text{-}p}$ et l'indicateur de performance "taux de faux négatifs (DPI)" $\varepsilon_{f\text{-}n}$ égal à zéro.

7.2 Modèles d'informations et de données

Dans le processus de développement par étapes des services de communication [b-UIT-T I.130], une distinction est faite entre les niveaux d'abstraction des "informations" et des "données" (par exemple les unités de données de protocole). Les modèles d'informations sont utilisés à un très haut niveau afin de décrire par exemple les flux d'informations entre les entités de réseau (voir par exemple [b-UIT-T I.130], [b-UIT-T X.1036]). Les modèles de données sont utilisés à un niveau inférieur afin de décrire par exemple un élément d'information du point de vue syntaxique (voir par exemple [b-UIT-T J.380.1]).

7.2.1 Modèle d'informations (exemple de cadre)

La spécification détaillée, quelle qu'elle soit, de la modélisation des informations concernant les règles de politique DPI et des flux d'informations n'a pas sa place dans une Recommandation "cadre". Toutefois, le document [b-IETF RFC 3060] peut par exemple servir de référence pour la modélisation des informations concernant les règles de politique DPI. Le Tableau 7-1 donne quelques exemples d'éléments d'information afin de donner des indications sur la manière dont un modèle concret pourrait être développé:

Tableau 7-1 – Exemple de modèle d'informations, basé sur le document [b-IETF RFC 3060]

Elément d'information (la présente Recommandation et la Recommandation [UIT-T Y.2770])	Modèle générique principal d'informations pour une politique conformément au document [b-IETF RFC 3060]
Règle de politique DPI	Pourrait reposer sur la classe "PolicyRule"
Combinaison de conditions de règle de politique DPI	Pourrait reposer sur la classe abstraite "PolicyCondition"
Condition unique de règle de politique DPI	Pourrait reposer sur la classe abstraite "PolicyCondition"
Action de règle de politique DPI	Pourrait reposer sur la classe abstraite "PolicyAction"
Ainsi de suite, par exemple le regroupement et la priorisation des règles de politique DPI, et des caractéristiques telles que la période de validité des règles, etc.	…

7.2.2 Modèle de données (exemple de cadre)

La spécification détaillée, quelle qu'elle soit, de la modélisation des objets de données concernant les règles de politique DPI n'a pas sa place dans une Recommandation "cadre" (car la porte serait ouverte au développement de la syntaxe de protocole).

Toutefois, le document [b-IETF RFC 4011] peut par exemple servir de référence pour la modélisation des données concernant les règles de politique DPI. Le Tableau 7-2 donne quelques exemples d'objets de données afin de donner des indications sur la manière dont un modèle concret pourrait être développé:

Tableau 7-2 – Exemple de modèle de données, basé sur le document [b-IETF RFC 4011]

Elément d'information (la présente Recommandation et la Recommandation [UIT-T Y.2770])	Objet de données générique, utilisant par exemple la base MIB de gestion basée sur la politique conformément à la norme [b-IETF RFC 4011]:
DPI-PIB	Pourrait reposer sur l'objet "pmPolicyTable", qui est lui-même lié à l'objet "pmPolicyCodeTable" (Note 1)
Règle de politique DPI, à savoir une entrée de la base DPI-PIB	Pourrait reposer sur l'objet "pmPolicyEntry"
Condition de règle de politique DPI	Pourrait reposer sur l'objet "pmPolicyCodeEntry" (Note 2)
Action de règle de politique DPI	Pourrait reposer sur l'objet "pmPolicyCodeEntry" (Note 2)
Etc.	Etc.
NOTE 1 – La représentation abstraite et la séparation de la "description de la règle" et du "code de la règle" dans deux tableaux associés permet de définir une base "DPI-PIB" efficace. NOTE 2 – En d'autres termes, la condition de règle et l'action de règle pourraient en fait utiliser le même modèle d'objet de données (dans cet exemple).	

Du point de vue des plans du réseau, on notera qu'un *objet de données* générique pourra être visible:

- en tant qu'objet géré du point de vue du plan de gestion DPI (voir l'interface e2 au § 8 de [UIT-T Y.2770]); et/ou
- en tant qu'objet commandé du point de vue du plan de commande DPI (voir l'interface e1 au § 8 de [UIT-T Y.2770]).

A titre d'exemple, une règle de politique DPI particulière pourrait être signalée (via e1) par l'entité DPI PD-FE, ou fournie (via e2) par un système de gestion DPI, mais conduire à une entrée de la base DPI-PIB "règle de politique DPI" correspondant à un seul et même objet.

7.3 Modèles de trafic

7.3.1 Introduction

Le présent paragraphe a pour objet de décrire certaines caractéristiques intéressantes des entités DPI (pour la définition, voir le § 3.2.7 de [UIT-T Y.2770]) du point de vue de la théorie du trafic. Cette description pourra faciliter ensuite la définition, par exemple, d'exigences fonctionnelles, de performance et de disponibilité, l'indication d'aspects architecturaux ou les évaluations de la performance.

Les modèles de trafic décrits ne sont que des exemples et ne sont pas nécessairement représentatifs d'une composante DPI donnée (DPI-PE, DPI-FE, moteur DPI, bibliothèque de signatures DPI, etc.).

7.3.2 Modèles de trafic de base pour le traitement sur le trajet des paquets

Le traitement du trafic se fait au niveau des paquets, ce qui correspond à la principale fonction d'une entité DPI-FE, et il est essentiellement réalisé par le moteur DPI imbriqué (pour la définition, voir le § 3.2.6 de [UIT-T Y.2770]).

Le moteur DPI est la composante principale d'une entité DPI-FE et il joue un rôle important dans ladite entité. Le trafic DPI est traité par le moteur DPI. Lors de la réalisation d'un moteur DPI sous la forme d'un composant physique, un traitement en parallèle peut aider à améliorer la performance du moteur DPI. Il pourrait par conséquent y avoir plusieurs unités de traitement à l'intérieur du composant physique correspondant à un moteur DPI.

7.3.2.1 Modèle de trafic de base d'une entité DPI-FE mettant l'accent sur le moteur DPI

La Figure 7-13 utilise l'exemple de modèle fonctionnel d'une entité DPI-FE illustré dans la Figure 6-1 de [UIT-T Y.2770] pour définir un modèle de trafic type. Pour le modèle de trafic, on s'intéresse uniquement au trajet des paquets, ce qui donne un modèle pour le moteur DPI.

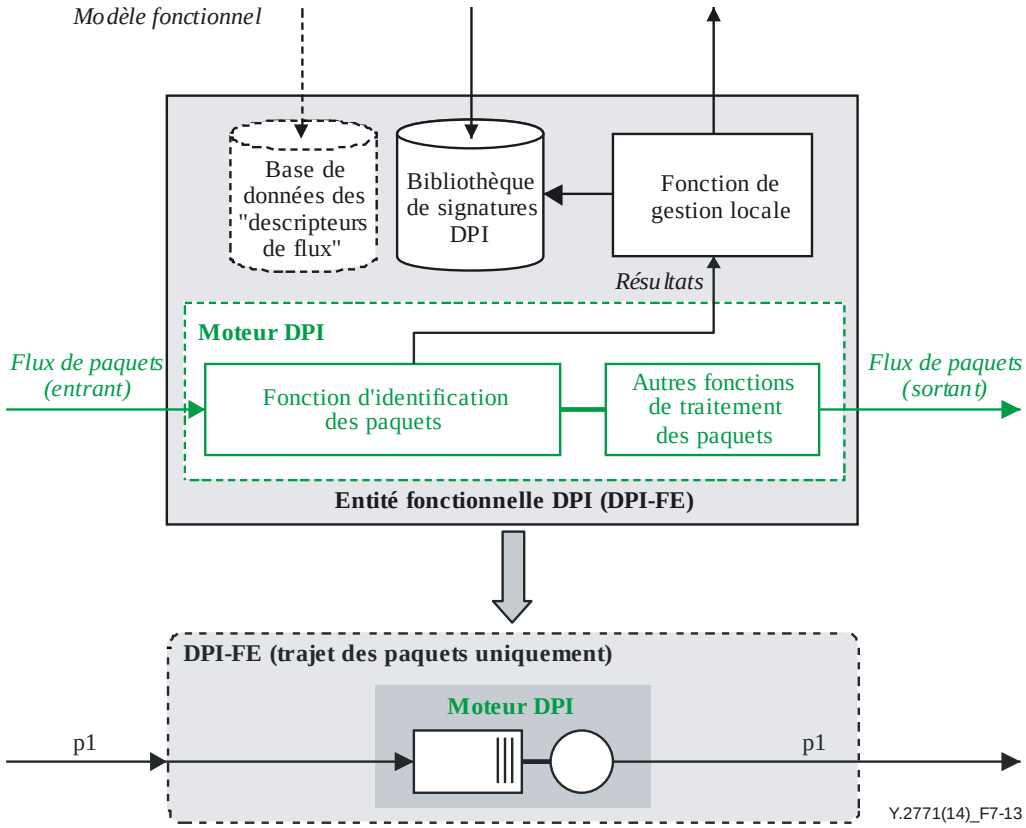


Figure 7-13 – Modèle de trafic de base d'une entité DPI-FE mettant l'accent sur le moteur DPI

Le modèle est caractérisé par un seul serveur et une file d'attente finie. Le serveur exécute donc toutes les fonctions sur le trajet des paquets. Le modèle avec un serveur à un étage représente un modèle de trafic pour un flux de paquets unidirectionnel.

7.3.2.2 Moteur DPI: extension au traitement sur le trajet des paquets en plusieurs étapes

7.3.2.2.1 Moteur DPI reposant sur un serveur à deux étages

La Figure 7-14 montre un exemple de modèle de trafic avec un moteur DPI à deux étages.

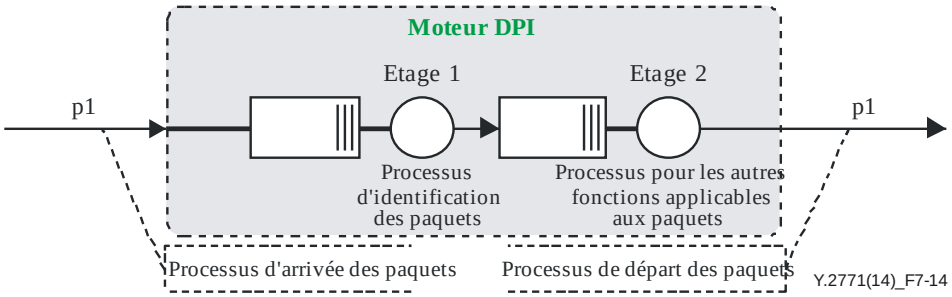


Figure 7-14 – Modèle de trafic avec moteur DPI: extension à un trajet des paquets en deux étapes

Dans cet exemple, le premier serveur est chargé du traitement des conditions de règle DPI.

7.3.2.2.2 Moteur DPI basé sur un serveur à 3 étages

Un moteur DPI pourrait être réalisé en interne sous la forme d'un système réparti, par exemple sous la forme d'une série d'éléments de traitement concaténés. Par exemple, le modèle fonctionnel illustré dans la Figure 7-3 représente trois étapes de traitement, appelées "balayage DPI", "analyse DPI" et "exécution d'action DPI", dont les abréviations sont respectivement DPI-ScF, DPI-AnF et DPI-AcEF.

La Figure 7-15 montre un exemple de modèle de trafic correspondant.

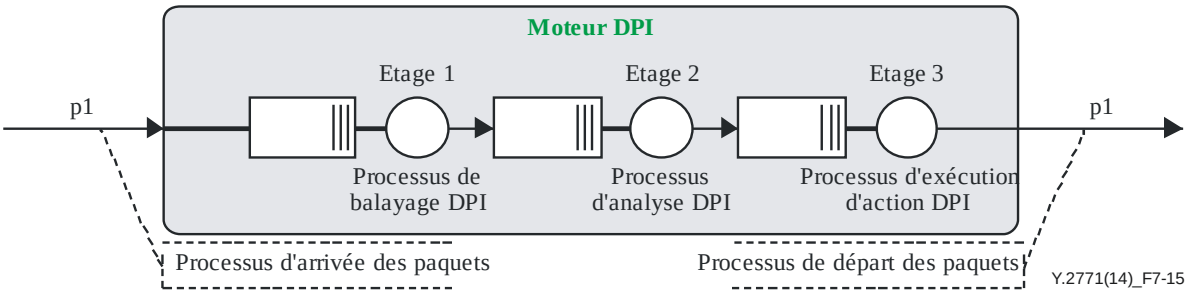


Figure 7-15 – Modèle de trafic avec moteur DPI: extension à un trajet des paquets en 3 étapes

7.3.3 Modèles de trafic étendus pour les moteurs DPI

7.3.3.1 Une seule interface externe et parallélisme interne

A titre d'exemple, il pourrait y avoir une entité DPI *hors du trajet* (voir le § 6.1) connectée via une route unique au réseau en mode paquet. Une telle entité DPI pourrait être chargée du traitement hors ligne d'un grand nombre de flux de paquets sélectionnés, auquel cas une grande capacité de traitement pourrait être requise. Le parallélisme pourrait être envisagé afin de fournir une grande capacité de traitement. La Figure 7-16 montre un exemple de modèle de trafic, avec plusieurs moteurs DPI en parallèle.

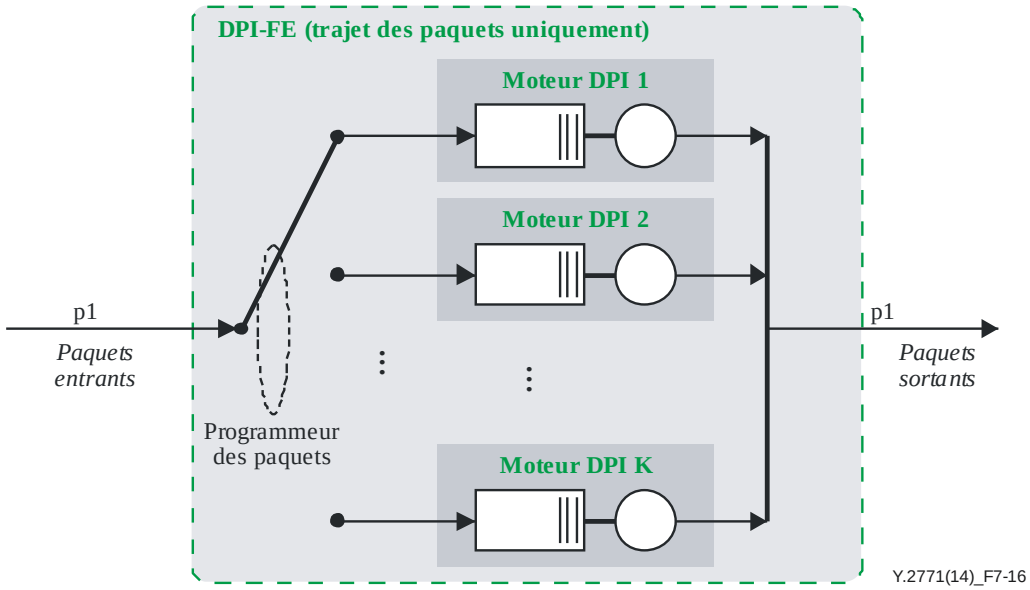


Figure 7-16 – Moteurs DPI – Une seule interface externe et parallélisme interne

Le modèle de trafic comporte une *fonction programmeur des paquets* pour l'attribution de chaque paquet entrant à un moteur DPI (serveur). Une telle fonction n'entre pas dans le cadre de la présente Recommandation.

NOTE – Par exemple, le programmeur des paquets pourrait:

a) être simplement un algorithme d'équilibrage de charge (autrement dit la programmation est basée uniquement sur la charge estimée des serveurs des moteurs DPI), ce qui n'a de sens que pour l'inspection DPI ne dépendant pas de l'état;

b) être fondé sur les informations du descripteur de flux (pour l'inspection DPI dépendant de l'état), mais on aurait alors, au minimum, un modèle de serveur à 2 étages pour ce qui est de la modélisation du trafic; ou

c) utiliser tout autre type de méthode de programmation.

7.3.3.2 Plusieurs interfaces externes et parallélisme interne

En règle générale, une entité DPI *sur le trajet* située dans le centre du réseau (voir le § 6.1) dispose de plusieurs interfaces *p1* physiques. Plusieurs moteurs DPI peuvent traiter en parallèle tous les flux de paquets entrants (voir la Figure 7-17). Il est généralement imposé que tous les moteurs DPI (par exemple *K*) soient connectés à *toutes* les interfaces p1 des paquets entrants (par exemple *N*). Pour cela, il faut donc prévoir une fonction de module de commutation de paquets *N-K*. Ce type de fonction n'entre pas dans le cadre de la présente Recommandation.

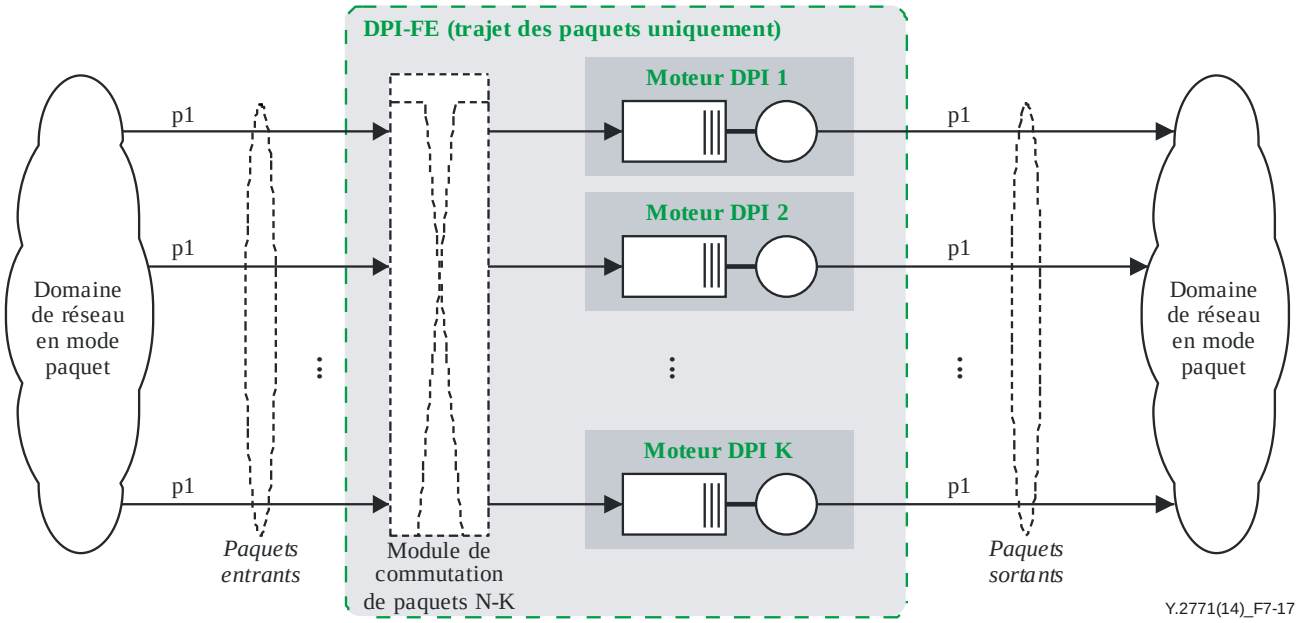


Figure 7-17 – Plusieurs interfaces externes et parallélisme interne

7.3.3.3 Moteurs DPI en parallèle basés sur des modèles de serveur à 3 étages

Les Figures 7-18 et 7-19 illustrent un modèle étendu, basé sur la combinaison de modèles de moteur DPI à 3 étages (§ 7.3.2.2.2) et sur un parallélisme au niveau des moteurs DPI (§ 7.3.3.1).

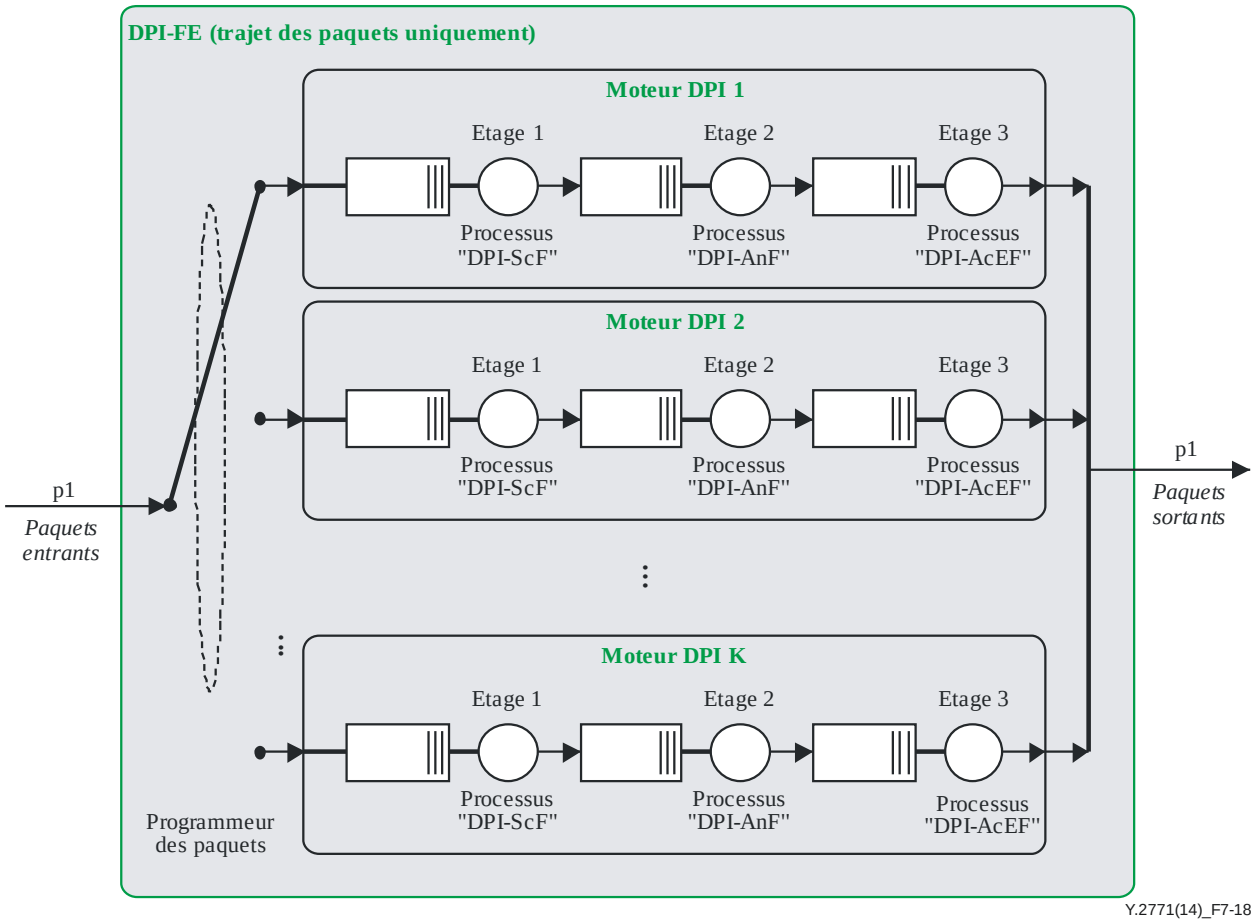


Figure 7-18 – Moteurs DPI en parallèle basés sur des modèles de serveur à 3 étages (une seule interface externe)

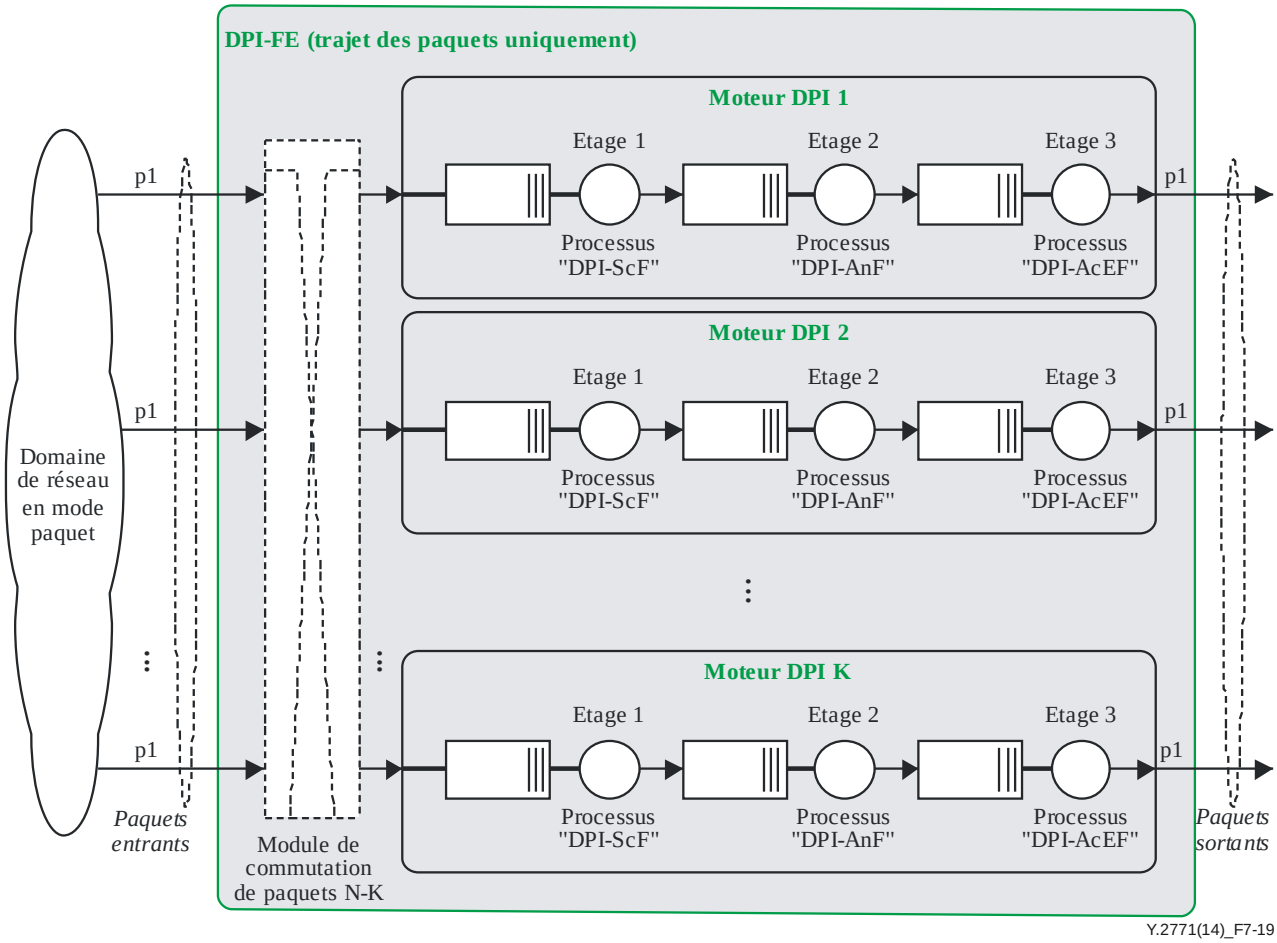


Figure 7-19 – Moteurs DPI en parallèle basés sur des modèles de serveur à 3 étages (plusieurs interfaces externes)

Les modèles de trafic sont caractérisés par des moteurs DPI qui fonctionnent complètement en parallèle, autrement dit sans aucune interdépendance. La performance maximale d'une telle architecture DPI-PE serait obtenue lorsque tous les serveurs sont "chargés de manière optimale" (c'est-à-dire lorsqu'aucun serveur n'est surchargé ou sous-chargé), ce qui suppose une répartition homogène de la charge dans les deux dimensions du modèle de trafic. Une telle architecture, plutôt difficile à concevoir, ne sera peut-être possible que pour certaines répartitions précises du trafic concernant la charge offerte en termes de paquets.

Ces considérations peuvent conduire à différentes architectures, telles que celles qui sont examinées dans le paragraphe qui suit.

7.3.3.4 Un seul moteur DPI à trois étages et parallélisme interne

Les Figures 7-20 et 7-21 illustrent un exemple d'un seul moteur DPI, basé sur trois étages de traitement et sur un parallélisme à chaque étage. Le niveau de parallélisme peut varier en fonction de l'étage, autrement dit le nombre de serveurs pourrait être différent à chaque étage (les valeurs de K1, K2 et K3 pourraient être différentes).

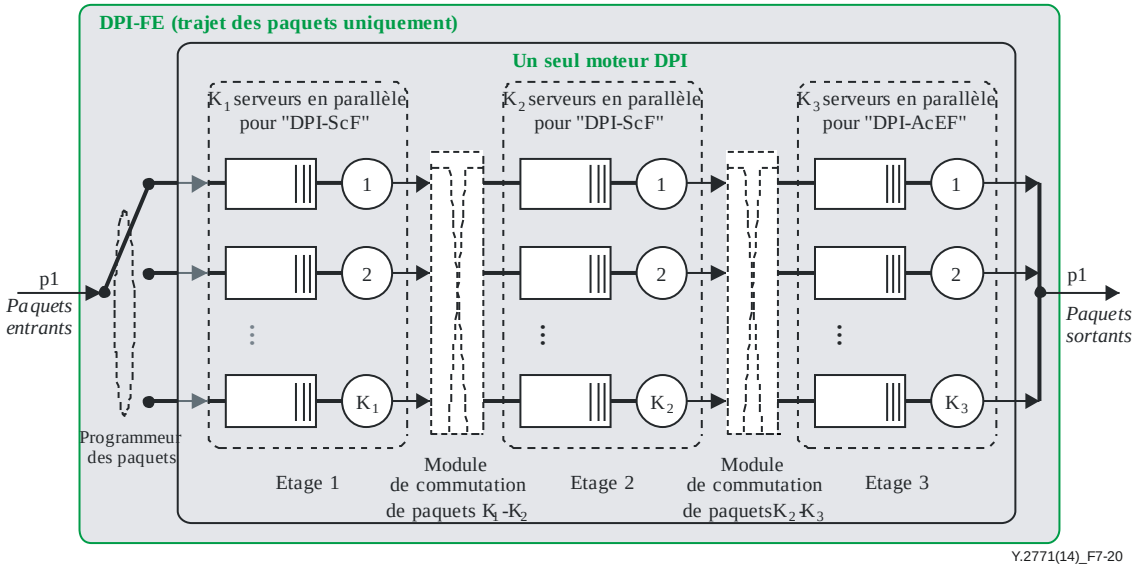


Figure 7-20 – Un seul moteur DPI à trois étages et parallélisme interne (une seule interface externe)

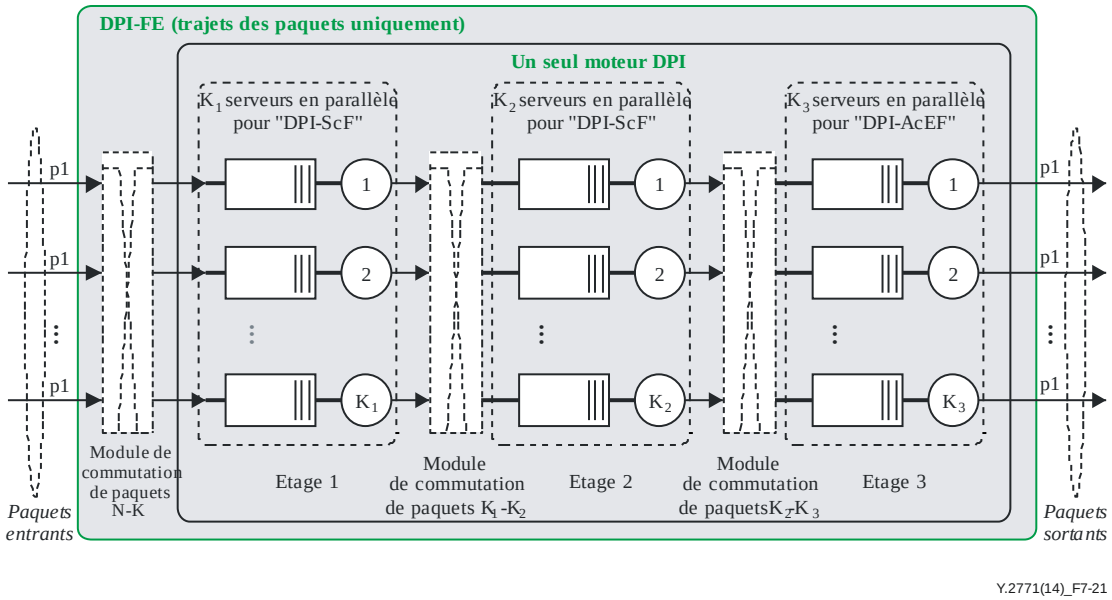


Figure 7-21 – Un seul moteur DPI à trois étages et parallélisme interne (plusieurs interfaces externes)

Lorsque le moteur DPI doit prendre en charge l'inspection DPI dépendant de l'état, il se peut que le routage de *tous* les paquets d'un *même flux* doive être assuré sur le même trajet de serveurs en raison des "informations d'état" locales. Cet aspect n'entre pas dans le cadre du modèle de trafic ci-dessus.

7.4 Identification des sous-composantes possibles d'une entité DPI-FE

Une entité DPI-FE peut être subdivisée en sous-composantes fonctionnelles, comme cela a déjà été illustré dans les modèles fonctionnels donnés en exemple dans les paragraphes précédents. Le Tableau 7-3 présente un aperçu des sous-composantes fonctionnelles types d'une entité DPI-FE. Il est fait référence en partie aux composantes dans les paragraphes qui suivent (par exemple dans le cas de l'examen des aspects de performance, des éventuelles exigences fonctionnelles ou opérationnelles, etc.).

Tableau 7-3 – Sous-composantes types d'une entité DPI-FE

Composante:	Description:
Fonction d'application de politique DPI (DPI-PEF):	Elément fonctionnel concernant l'application des règles de politique DPI, qui contient au moins une base d'informations de politique DPI, une fonction d'identification des paquets DPI et une fonction d'exécution d'action DPI.
Description plus détaillée de la fonction DPI-PEF: 1) Trajet de traitement des paquets	
1.1) Fonction d'identification des paquets DPI (DPI-PIF) Exemple de décomposition fonctionnelle:	Elément fonctionnel chargé d'appliquer les conditions de politique DPI aux paquets entrants.
Fonction de balayage DPI (DPI-ScF):	Elément fonctionnel (faisant partie de la fonction DPI-PIF) qui exécute les fonctions de comparaison initiales, déterminées par les conditions de règle de politique DPI.
Fonction d'analyse DPI (DPI-AnF):	Elément fonctionnel (faisant partie de la fonction DPI-PIF) qui exécute les fonctions de comparaison suivantes, également déterminées par les conditions de règle de politique DPI (par exemple relatives aux éléments d'en-tête de paquet ou au contenu (données utiles des paquets)).
1.2) fonction d'exécution d'action DPI (DPI-AcEF):	Elément fonctionnel qui exécute des opérations sur certains paquets, en fonction des actions de règle de politique DPI identifiées.
2) fonction de base d'informations de politique DPI (DPI-PIB; NOTE 1):	Elément fonctionnel représentant une base de données, qui contient un ensemble d'une ou de plusieurs entrées concernant les règles de politique DPI (voir ci-dessous).
a) entrée concernant une règle de politique DPI:	Entrée d'une table qui contient une règle de politique DPI (Note 2).
i) condition de règle de politique DPI (ou "condition concernant une règle"):	Expression (en général de type booléen). Une condition est également appelée critère de concordance (par exemple en raison des types de condition représentant une concordance partielle, une concordance totale, une concordance de préfixe, une concordance de préfixe le plus long, etc.)
ii) action de règle de politique DPI (ou "action de règle"):	Action exécutée après l'évaluation de toutes les conditions de politique propres à une règle et la décision d'exécuter cette action.
NOTE 1 – Egalement appelée *table des règles*, *bibliothèque des signatures de politique* ou simplement *bibliothèque de signatures*. NOTE 2 – Une ou plusieurs règles pourraient être appliquées. Ces règles peuvent être prédéfinies statiquement (via la gestion de la configuration du nœud en mode paquet, appelée gestion de politique DPI), ou signalées (via une interface de commande de politique) ou générées dynamiquement au niveau local (via une fonction PDF locale). Les règles de politique DPI sont utilisées pour comparer les informations de commande de protocole (PCI, à savoir des éléments d'en-tête de paquet) ou les données utiles/le contenu des flux de paquets avec un ensemble de conditions pour déterminer s'il y a ou non concordance de chaîne.	

7.5 Modèles de tolérance aux dérangements

La fiabilité et la disponibilité d'un nœud de réseau (par exemple un nœud DPI) sont très importantes pour le réseau dans lequel le nœud de réseau est déployé. Lorsque le nœud de réseau est hors service (voir par exemple le modèle d'états opérationnels dans la Recommandation [UIT-T X.731]), cette situation pourrait entraîner un désastre dans le réseau, pouvant obliger tous les utilisateurs du réseau à passer en mode hors ligne. Il en résulterait une perte massive d'informations précieuses. Il est donc essentiel de faire en sorte que les nœuds de réseau présentent une fiabilité et une disponibilité élevées. En tant que nœud de réseau, un nœud DPI devrait aussi présenter une fiabilité et une disponibilité élevées.

En utilisant une méthode de tolérance aux dérangements, le groupe de redondance "1+N" DPI vise à améliorer la fiabilité et la disponibilité du réseau déployé avec des nœuds DPI.

La fiabilité du groupe de redondance "1+N" DPI peut être calculée à l'aide des paramètres suivants:

1) MTBF (durée moyenne entre deux pannes): durée moyenne entre deux pannes du groupe de redondance "1+N" DPI.

2) MTTR (durée moyenne de réparation): temps mis pour assurer le retour à un fonctionnement normal du groupe de redondance "1+N" DPI en panne.

La disponibilité d'un groupe de redondance "1+N" DPI peut être calculée à l'aide des formules suivantes (voir la Recommandation [UIT-T G.602]):

3) Disponibilité = durée de disponibilité/(durée d'indisponibilité + durée de disponibilité) ou

4) Disponibilité = MTBF/(MTBF + MTTR)

5) A l'intérieur d'un groupe de redondance "1+N" DPI, le nombre de composants fonctionnels redondants dépend de la réalisation particulière et n'entre pas dans le cadre de la présente Recommandation. A l'intérieur d'un groupe de redondance, les composants fonctionnels sont soit en mode actif soit en mode secours, un seul étant un composant fonctionnel actif, les autres étant des composants fonctionnels de secours. Lorsque le composant fonctionnel actif est hors service, un seul des composants fonctionnels de secours deviendra le nouveau composant fonctionnel actif et l'ancien composant fonctionnel actif passera en mode secours.

6) L'interface entre le composant fonctionnel actif et un composant fonctionnel de secours, qui est utilisée pour le basculement de l'un à l'autre, est indépendante de l'inspection DPI et propre à la mise en œuvre; elle n'entre donc pas dans le cadre de la présente Recommandation.

7) Plusieurs modèles de tolérance aux dérangements sont présentés, à savoir le modèle de tolérance aux dérangements au niveau du nœud DPI (§ 7.5.1), le modèle de tolérance aux dérangements au niveau de la fonction DPI-PEF (§ 7.5.2), le modèle de tolérance aux dérangements au niveau de la base DPI-PIB (§ 7.5.3) et le modèle de tolérance aux dérangements au niveau du moteur DPI (§ 7.5.4).

8) Tous les modèles de tolérance aux dérangements sont basés sur un groupe de redondance "1+N" DPI (en d'autres termes, sur une redondance des composants fonctionnels, par exemple nœuds DPI dans la Figure 7-22).

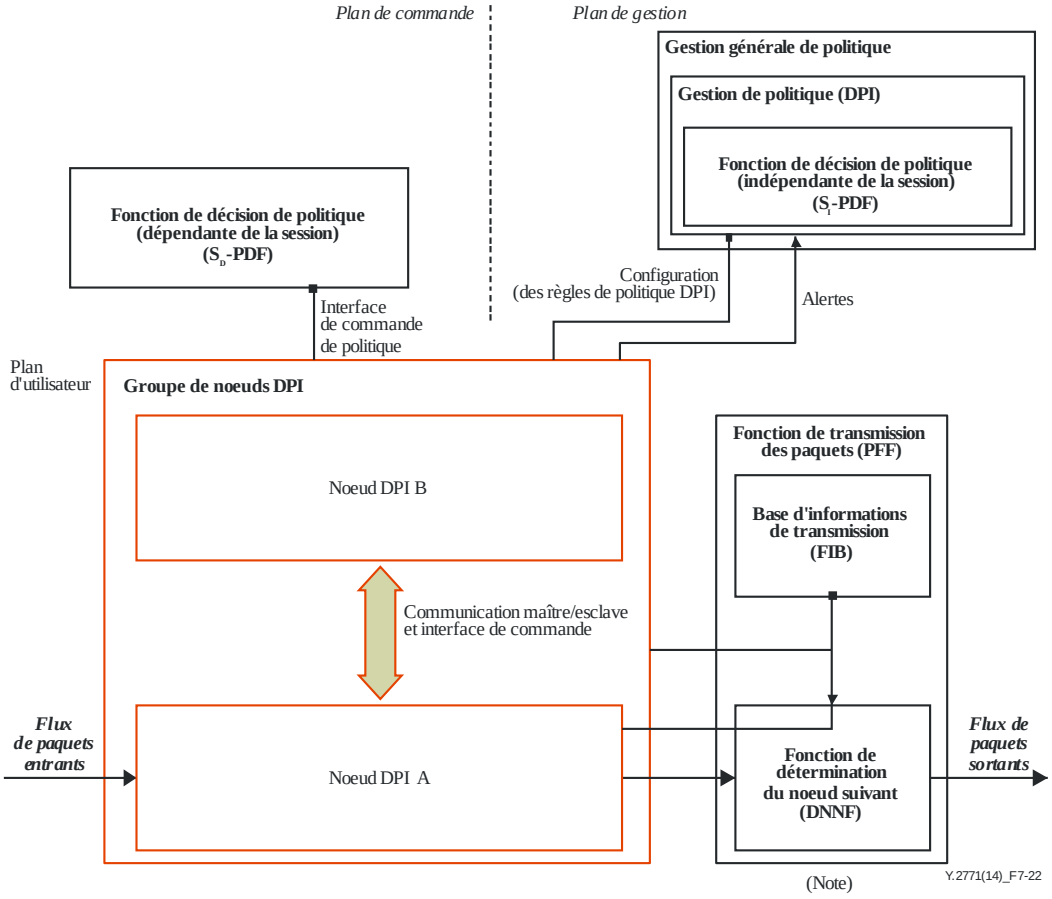
9) Le composant fonctionnel actif et les composants fonctionnels de secours devraient conserver des informations totalement identiques (base PIB par exemple) via une méthode de synchronisation des données, laquelle dépend de la réalisation particulière et n'entre pas dans le cadre de la présente Recommandation.

7.5.1 Modèle de tolérance aux dérangements au niveau du nœud DPI

La Figure 7-22 illustre un modèle DPI avec garantie de fiabilité au niveau du nœud DPI, dans lequel deux nœuds DPI ou plus sont déployés ensemble pour former un groupe de nœuds DPI (un groupe de redondance "1+N" DPI dans lequel les nœuds DPI sont les composants fonctionnels), l'un des nœuds étant le nœud DPI actif, les autres étant des nœuds DPI de secours. Par ailleurs, le nœud DPI

actif et les nœuds DPI de secours doivent dupliquer les informations internes comme requis pour le fonctionnement normal. Dès que le nœud DPI actif est hors service, l'un des nœuds DPI de secours deviendra automatiquement le nœud DPI actif.

Seuls deux nœuds DPI sont illustrés dans la Figure 7-22, mais le modèle de tolérance aux dérangements est analogue lorsqu'il y a plus de deux nœuds DPI (concept de redondance "1+N").



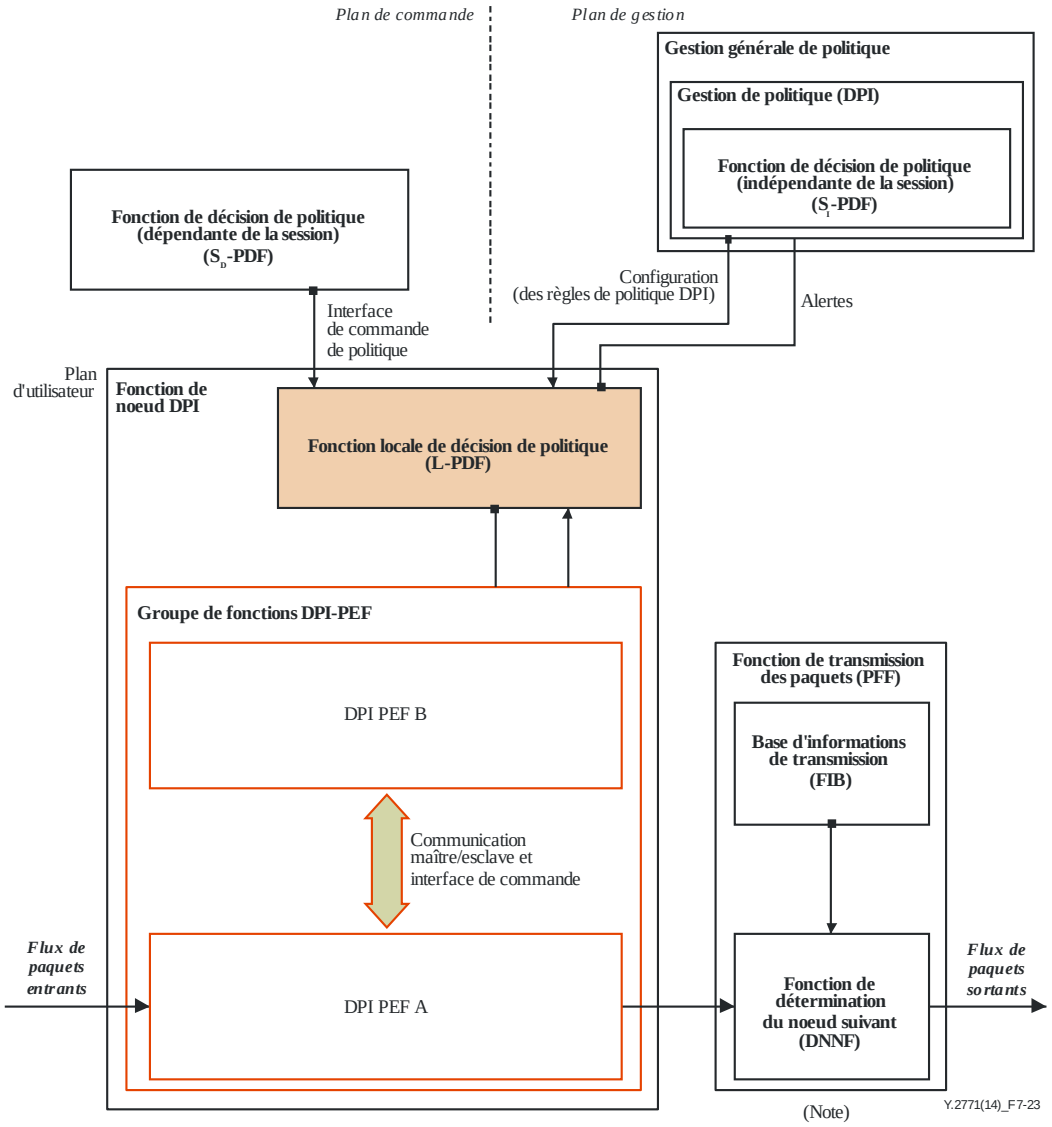
NOTE – La fonction PFF n'entre pas dans le cadre de la présente Recommandation.

Figure 7-22 – Modèle DPI avec garantie de fiabilité au niveau du nœud DPI

7.5.2 Modèle de tolérance aux dérangements au niveau de la fonction DPI-PEF

La Figure 7-23 illustre un modèle DPI avec prise en charge de la fiabilité au niveau de la fonction DPI-PEF; deux composants DPI-PEF ou plus (en d'autres termes, un groupe de redondance "1+N" DPI dans lequel les composants DPI-PEF sont les composants fonctionnels) sont prévus à l'intérieur d'un nœud DPI, l'un des composants étant le composant actif, les autres étant les composants de secours. Les procédures de basculement en cas de panne sont analogues à ce qu'elles sont dans le cas de la prise en charge de la fiabilité au niveau du nœud (voir le § 7.5.1).

Seuls deux composants PEF sont illustrés dans la Figure 7-23, mais le modèle de tolérance aux dérangements est analogue lorsqu'il y a plus de deux composants PEF.



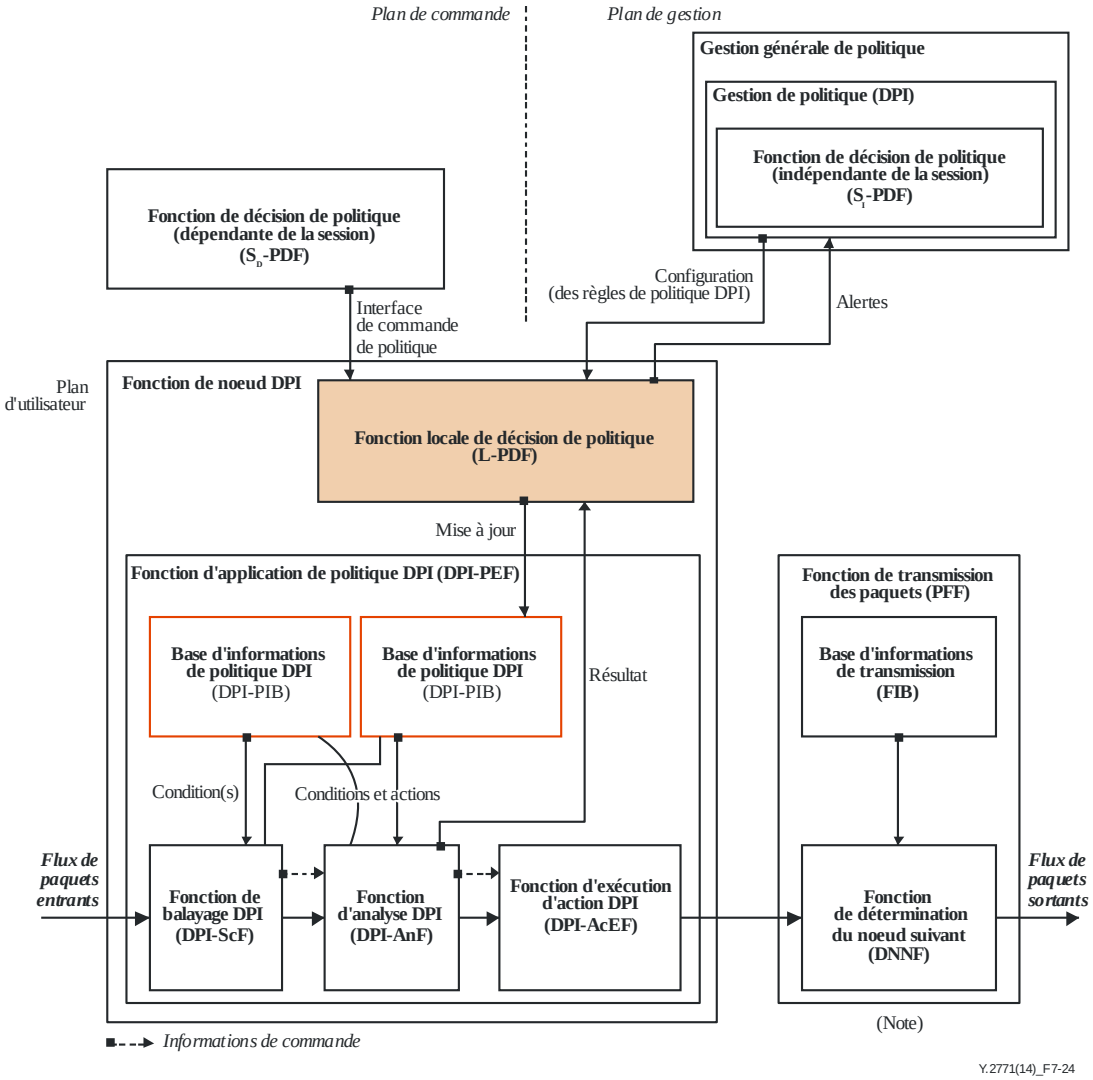
NOTE – La fonction PFF n'entre pas dans le cadre de la présente Recommandation.

Figure 7-23 – Modèle DPI avec prise en charge de la fiabilité au niveau de la fonction DPI-PEF

7.5.3 Modèle de tolérance aux dérangements au niveau de la base DPI-PIB

La Figure 7-24 illustre un modèle DPI avec prise en charge de la fiabilité au niveau de la base DPI-PIB; deux exemplaires ou plus de la base DPI-PIB (en d'autres termes, deux exemplaires ou plus de la base DPI-PIB constituent un groupe de redondance "1+N" DPI) se trouvent dans un nœud DPI, et toutes les bases DPI-PIB sont synchronisées et contiennent donc des informations identiques. L'une des bases DPI-PIB a le rôle actif, les autres ayant un rôle de secours. Dès que la base PIB active est hors service, l'une des bases PIB de secours deviendra automatiquement la base PIB active.

Seules deux bases DPI-PIB sont illustrées dans la Figure 7-24, mais le modèle de tolérance aux dérangements est analogue lorsqu'il y a plus de deux bases DPI-PIB.



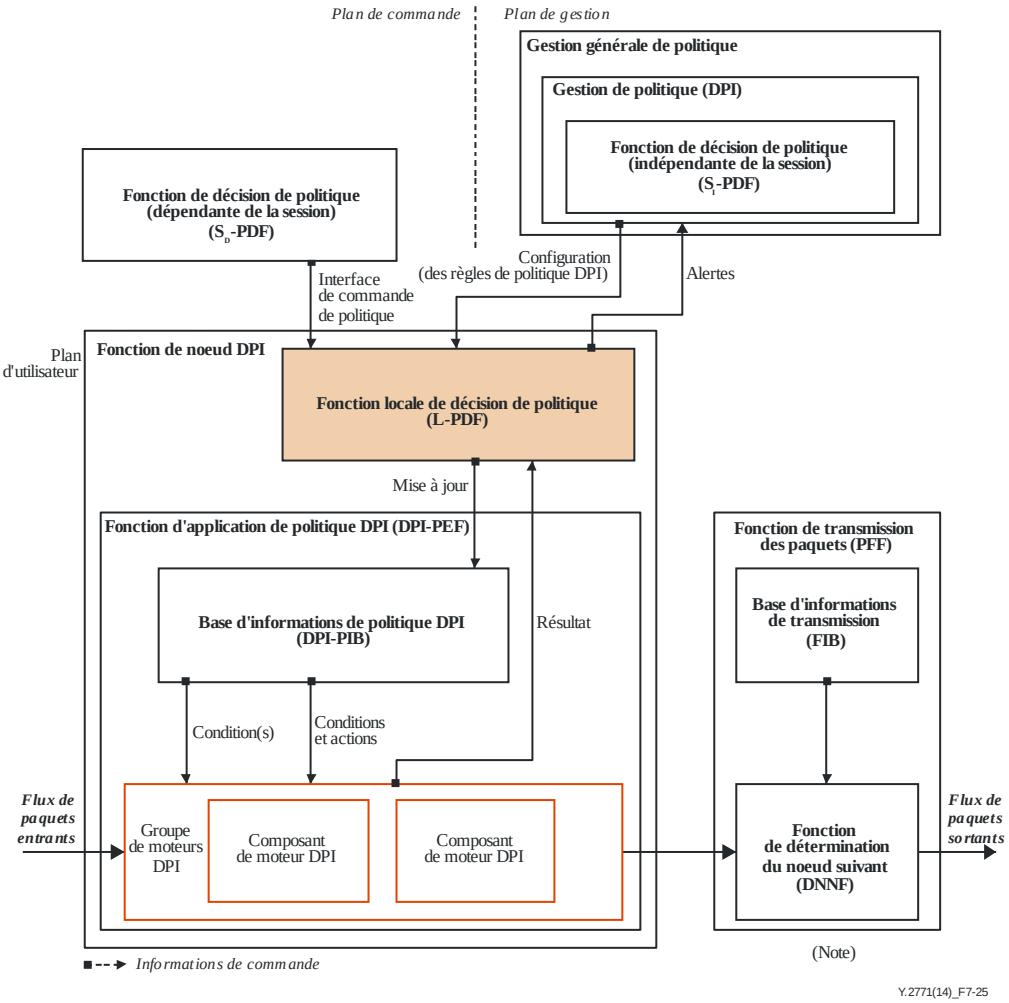
NOTE – La fonction PFF n'entre pas dans le cadre de la présente Recommandation.

Figure 7-24 – Modèle DPI avec garantie de fiabilité au niveau de la base DPI-PIB

7.5.4 Modèle de tolérance aux dérangements au niveau du moteur DPI

La Figure 7-25 illustre un modèle DPI avec prise en charge de la fiabilité au niveau du moteur DPI. Les principes de tolérance aux dérangements sont les mêmes que dans le cas des modèles précédents aux niveaux plus élevés.

Seuls deux composants de moteur DPI sont illustrés dans la Figure 7-25, mais le modèle de tolérance aux dérangements est analogue lorsqu'il y a plus de deux composants de moteur DPI.



NOTE – La fonction PFF n'entre pas dans le cadre de la présente Recommandation.

Figure 7-25 – Modèle DPI avec garantie de fiabilité au niveau du moteur DPI

8 Cadre de performance

8.1 Objet et portée des considérations relatives à la performance

Le présent paragraphe décrit un cadre et un procédé pour l'identification et l'élaboration d'indicateurs de performance relatifs à l'inspection DPI. Ces indicateurs peuvent être utilisés pour caractériser le comportement des entités DPI.

Le cadre de performance porte essentiellement sur:

1) Les indicateurs de performance:

   La capacité, la disponibilité et la performance d'une entité DPI peuvent être caractérisées par des indicateurs de performance. L'objectif premier est:

   a) de préciser si les indicateurs de performance existants, non-DPI, pourraient être réutilisés;

   b) de reconnaître les indicateurs de performance propres à l'inspection DPI, qui sont déjà utilisés par d'autres organisations s'occupant d'inspection DPI;

   c) d'identifier de nouveaux indicateurs de performance propres à l'inspection DPI, ce qui implique de définir ces indicateurs; et

   d) de déterminer si les indicateurs sont des indicateurs fondamentaux de performance (KPI) ou d'autres indicateurs.

2) Les exigences de performance:

Les exigences DPI en question sont associées aux différents indicateurs de performance. Les exigences de performance qui dépendent de la mise en œuvre n'entrent pas dans le cadre de la présente Recommandation. Par conséquent, il est possible d'énoncer des exigences de performance qualitatives ou relatives, mais la spécification d'exigences de performance quantitatives ou absolues n'est possible que dans certains cas limités (par exemple si la valeur maximale prévue du temps de transfert interne au nœud dépend de considérations générales relatives au réseau de bout en bout…).

3) Les repères de performance:

L'établissement de repères est relativement difficile en ce qui concerne l'identification et la spécification de scénarios de référence bien reconnus et significatifs. La définition de repères de performance DPI n'entre pas dans le cadre de la présente Recommandation. Toutefois, la présente Recommandation pourrait donner des informations et des indications sur les aspects à prendre en compte lorsqu'on cherche à spécifier un repère de performance pour les entités DPI.

Pour définir de nouveaux types d'indicateurs de performance, il convient de suivre les lignes directrices énoncées dans la référence [b-IETF RFC 6390]; il s'agit donc essentiellement de faire figurer au moins les éléments suivants:

- nom et description de l'indicateur;
- méthode de mesure ou de calcul;
- unité de mesure; et
- une définition de l'indicateur de performance, qui ne doit pas être liée à un paramètre statistique tel qu'une valeur minimale, une valeur maximale, une moyenne, une fonction de distribution de probabilité, une variance, etc. Ces aspects concernent plutôt la spécification des exigences.

8.2 Indicateurs de performance

8.2.1 Aperçu – Indicateurs de performance pour les nœuds DPI

Les exigences de performance sont liées aux indicateurs de performance. Les indicateurs essentiels sont appelés indicateurs fondamentaux de performance (KPI); ils représentent un sous-ensemble de l'ensemble général des indicateurs.

8.2.1.1 Lignes directrices pour déterminer si les indicateurs de performance liés à l'inspection DPI sont des indicateurs KPI ou non

La présente Recommandation définit comme suit les indicateurs KPI (NOTE 1 – D'après la référence [ETSI TS 132.410]):

- **Indicateurs fondamentaux de performance (KPI) en général:**

  Ce sont les principaux indicateurs utilisés pour évaluer la performance d'un processus en tant qu'indicateurs relatifs à la fonction centrale de l'élément de réseau.

- **Indicateurs fondamentaux de performance pour les entités DPI (KPI_{DPI})**:

  Un indicateur KPI_{DPI} – tel qu'utilisé dans le cadre de la présente Recommandation – caractérise donc la performance du moteur DPI (voir le § 3.2.6 de [UIT-T Y.2770]; également appelé trajet de traitement des paquets DPI).

NOTE 2 – Dans la présente Recommandation, l'indicateur de performance a deux équivalents en anglais: performance indicator et performance metric.

Afin de déterminer si les indicateurs de performance DPI sont ou non des indicateurs KPI, il convient de prendre en considération les critères suivants. Un indicateur KPI pour les entités DPI devrait remplir les conditions suivantes:

1) l'indicateur de performance devrait être lié au trajet de traitement des paquets proprement dit, les règles de politique DPI étant appliquées aux objets que sont les paquets (et donc ne pas être lié à quelque autre fonction DPI que ce soit en dehors du trajet des paquets DPI); et

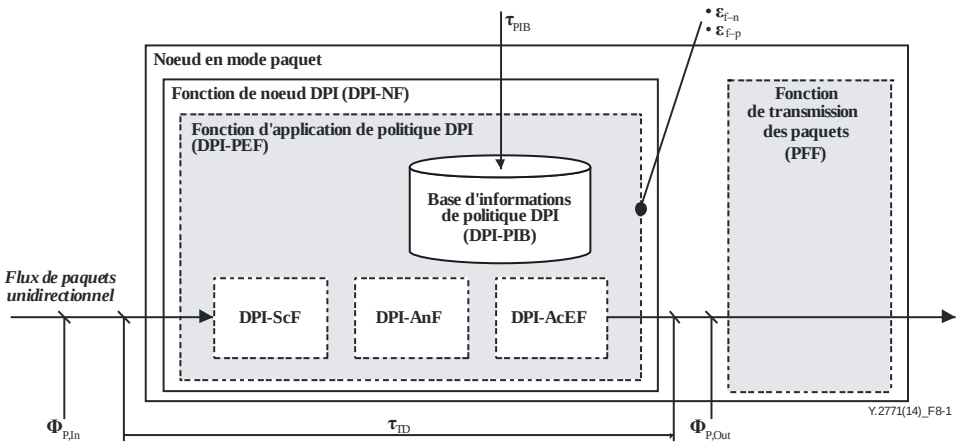
2) l'indicateur de performance devrait être indépendant du cas d'utilisation DPI (et donc ne pas être propre à une application liée à des services DPI particuliers); et

3) l'indicateur de performance devrait être indépendant des protocoles particuliers au-dessous ou au-dessus de la couche IP (et donc, par exemple, ne pas être propre à un protocole de transport IP (tel que TCP) ou à un protocole d'application IP particulier); et

4) l'indicateur de performance devrait être indépendant des réalisations physiques des entités DPI (et donc ne pas être lié à des aspects propres à la mise en œuvre tels que la consommation d'énergie, la dissipation d'énergie, des composants de traitement de pointe, etc.).

8.2.1.2 Indicateurs fondamentaux de performance types pour les nœuds DPI

La Figure 8-1 illustre certains exemples bien connus d'indicateurs KPI pour les nœuds DPI (la liste des indicateurs KPI_{DPI} n'est pas exhaustive). Les indicateurs KPI_{DPI} types sont énumérés après la figure. Les (éventuelles) exigences de performance correspondantes sont décrites dans des paragraphes distincts.



NOTE 1 – Le nœud en mode paquet et la fonction PFF apparaissent afin de spécifier sans ambiguïté les indicateurs de performance, mais les deux entités en tant que telles n'entrent pas dans le cadre de la présente Recommandation.
NOTE 2 – La fonction PFF n'est présente que pour le mode DPI sur le trajet.

Figure 8-1 – Aperçu – Indicateurs fondamentaux de performance pour les nœuds DPI

Les principaux indicateurs de performance types sont les suivants:

- KPI "**temps de transfert interne au nœud** (DPI)" τ_{TD} [µs]: voir le § 8.2.3.1.
- KPI "**débit de traitement des paquets** (DPI)" $\phi_{P,In}[s^{-1}]$: voir le § 8.2.3.2.
- KPI "**taux d'erreurs** (DPI)" ε_{DPI}: voir le § 8.2.3.3.
  - KPI "taux de faux positifs (DPI)" $\varepsilon_{f\text{-}p}$.
  - KPI "taux de faux négatifs(DPI)" $\varepsilon_{f\text{-}n}$.
- KPI "**Débit des paquets identifiés avec succès** (DPI)" $\phi_{P,Identified}[s^{-1}]$: voir le § 8.2.3.4.

8.2.2 Gabarit formel pour les définitions des indicateurs de performance

Dans la présente Recommandation, les indicateurs de performance sont définis conformément au gabarit présenté dans le Tableau 8-1, qui est déduit du gabarit de l'IETF présenté au § 5.4.4 de [b-IETF RFC 6390] (*Performance Metric Definition Template*).

Tableau 8-1 – Gabarit formel pour les définitions des indicateurs de performance

Nom de l'indicateur:	N	
Symbole:	I	
Description de l'indicateur:	N	
Méthode de mesure ou de calcul:	N	
Unité de mesure:	N	
Point(s) de mesure avec domaine de mesure potentiel:	N	
Intervalle de mesure:	N	
Mise en œuvre:	I	
Vérification:	I	
Utilisation et applications:	I	Par exemple "DPI en temps réel", "DPI pas en temps réel"
Modèle de notification:	I	
Type "KPI": oui/non?	I	A savoir "KPI", "non-KPI" ou "indéterminé"
NOTE – Eléments de description normatifs (N) et informatifs (I).		

Le gabarit est utilisé afin de garantir une qualité minimale de spécification pour les indicateurs définis dans la présente Recommandation. Toutefois, la présente Recommandation fournit essentiellement les éléments de description *normatifs*, car il s'agit d'une Recommandation "cadre". Les éléments de description (*informatifs*) vides indiquent que l'utilisation de l'indicateur en question dans une spécification de performance réelle nécessiterait d'abord un travail de spécification complémentaire afin d'obtenir un indicateur applicable complet. A titre d'exemple, l'élément de description "Mise en œuvre" n'a pas à être spécifié dans une Recommandation "cadre", ou la définition d'un indicateur sans l'élément "Vérification" est inutile (en effet, cet élément est nécessaire pour l'étalonnage de la fonction de mesure).

8.2.3 Définitions d'indicateurs de performance généraux pour les entités DPI

8.2.3.1 Indicateur DPI "temps de transfert interne au nœud"

Les règles de politique relatives à l'inspection DPI sont appliquées à chacun des paquets d'un flux donné. Ce type d'application de politique introduit un temps de service et d'attente supplémentaire sur le trajet de transmission des paquets au niveau d'un nœud en mode paquet (par exemple un saut IP) avec prise en charge d'un "moteur DPI" (à savoir un point d'application de politique (PEP) assurant l'inspection DPI). L'indicateur de performance *temps de transfert interne au nœud* représente le temps de transfert des paquets par l'élément de réseau proprement dit.

Le Tableau 8-2 contient la définition de l'indicateur.

Tableau 8-2 – Indicateur DPI "Temps de transfert interne au nœud"

Nom de l'indicateur:	N	Temps de transfert interne au nœud
Symbole:	I	τ_{TD}
Description de l'indicateur:	N	Temps d'attente et de service cumulés pour un paquet dans un nœud DPI.
Méthode de mesure ou de calcul:	N	Pour calculer cette valeur, on relève l'heure d'entrée et l'heure de sortie ($T_{in,i}$ et $T_{out,i}$) de chaque paquet aux interfaces d'une représentation physique ou logique d'une fonction de nœud DPI. Condition préalable: l'entité de mesure doit pouvoir identifier les différents paquets. Avertissement: cet indicateur dépend en principe de la charge car le *temps de transfert* interne au nœud est composé d'un *temps de service* et d'un *temps d'attente* internes au nœud. La charge, ou plus précisément la charge soumise au traitement DPI $A_{DPI\text{-}NF}$, est fonction du débit de paquets entrants $\phi_{P,In}$ et du temps moyen de service par paquet $T_{H,Packet}$, à savoir: $A_{DPI-NF} = \phi_{P,In} \cdot T_{H,Packet}$ Dépendance principale vis-à-vis de la charge (voir aussi le § 8.3): $\tau_{TD} = f(A_{DPI-NF})$
Unité de mesure:	N	ns
Point(s) de mesure avec domaine de mesure potentiel:	N	Voir la Figure 8-1 (modèle de trafic).
Intervalle de mesure:	N	Cet indicateur peut être utilisé sur un large éventail d'intervalles de temps.
Mise en œuvre:	I	–
Vérification:	I	–
Utilisation et applications:	I	"DPI en temps réel"
Modèle de notification:	I	Généralement dans le cadre de la gestion de la performance
Type "KPI": oui/non?	I	"KPI"
NOTE – N: élément de description normatif; I: élément de description informatif.		

8.2.3.1.1 Analyse complémentaire

a) Nœuds DPI ou nœuds non-DPI:

Exemple du nœud IP: le temps de transfert dans un nœud DPI peut, à la base, être supérieur au temps de transfert dans un nœud IP existant (à savoir un saut IP ou un routeur conformément à la référence [IETF RFC 1812]) en raison de la fonction de service supplémentaire venant s'ajouter à la fonctionnalité de transmission IP native.

b) Relations types:

Le temps de transfert interne au nœud, τ_{TD}, pourrait aussi dépendre (car il est propre à la mise en œuvre) des paramètres suivants:

– Le nombre de règles de politique DPI N_{db} (par exemple augmentation du temps de service lorsque plusieurs règles de politique DPI sont traitées en série),

– La taille de paquet *Sp*[bit] (par exemple augmentation du temps de recherche ou de comparaison dans le cadre de la vérification des conditions de politique DPI), cette taille pouvant être liée à la valeur de la taille de trame L2 donnée par la référence [b-IETF RFC 2544], et

– Le nombre de moteurs DPI N_{DPIeng} (par exemple cas du parallélisme interne, voir le § 7.3.3).

Ainsi, dans cet exemple, τ_{TD} serait fonction des paramètres *Ndb, Sp* et N_{DPIeng}, à savoir:

$$\tau_{TD} = f(N_{db}, S_P, N_{DPIeng})$$

Les trois paramètres ont donc une incidence sur le temps moyen de service par paquet $T_{H,Packet}$ (présenté dans le Tableau 8-3): les deux premiers paramètres sont des facteurs d'augmentation, tandis que le troisième paramètre conduit à une réduction du temps moyen de service.

c) Exigence de performance qualitative:

Le temps de transfert (y compris le temps de service supplémentaire dû au traitement DPI) devrait respecter les exigences de temps réel de bout en bout relatives au service de communication d'ensemble.

NOTE 1 – Cette capacité de transmission des paquets est également communément appelée "traitement à la vitesse filaire".

NOTE 2 – Un tel objectif de performance peut limiter le nombre de règles de politique appliquées à chaque paquet (simplement en raison du temps de service limité qui est prévu).

8.2.3.2 Indicateur DPI "débit de traitement des paquets"

Le Tableau 8-3 contient la définition de l'indicateur.

Tableau 8-3 – Indicateur DPI "Débit de traitement des paquets"

Nom de l'indicateur:	N	Débit de traitement des paquets
Symbole:	I	$\phi_{P,In}$
Description de l'indicateur:	N	Le débit auquel les paquets sont traités par la fonction DPI-PEF. Il s'agit du débit de paquets à l'entrée car les règles de politique DPI sont appliquées à chaque paquet entrant. Le débit de sortie est égal ou inférieur au débit d'entrée (en raison des éventuelles actions d'élimination de paquets), $\boxed{\phi_{P,In} \leq \phi_{P,Out}}$
Méthode de mesure ou de calcul:	N	Décompte de tous les paquets observés à l'interface d'entrée *p1* pendant une certaine durée. Pour calculer la valeur, on divise alors le nombre de paquets par la durée.
Unité de mesure:	N	s^{-1}
Point(s) de mesure avec domaine de mesure potentiel:	N	Voir la Figure 8-1 (modèle de trafic).
Intervalle de mesure:	N	Cet indicateur peut en principe être utilisé sur un large éventail d'intervalles de temps. En général, on utilise une échelle de temps de l'ordre de la seconde.
Mise en œuvre:	I	–
Vérification:	I	–
Utilisation et applications:	I	"DPI en temps réel"
Modèle de notification:	I	Généralement dans le cadre de la gestion de la performance
Type "KPI": oui/non?	I	"KPI"
NOTE – N: élément de description normatif; I: élément de description informatif.		

Le débit de traitement des paquets DPI, ϕ_P, dépend de nombreux paramètres, par exemple de la combinaison:

– du nombre de règles de politique DPI, ou de la taille de la base DPI-PIB, *Ndb*;

– de la taille de paquet, *Sp,* cette taille pouvant être liée aux valeurs de la taille de trame L2 données dans la référence [b-IETF RFC 2544]; et

– d'éventuels autres paramètres.

Exemple: Lorsque $(\phi_P, N_{db,} Sp) = (200, 1000, 64)$, le débit de traitement est d'au moins 200 paquets/s lorsque le nombre de règles de politique est inférieur à 1000 et que la taille de paquet est de 64.

Le comportement qualitatif est décrit au § 8.3. La mise à jour de la base DPI-PIB moyennant l'ajout de nouvelles règles de politique DPI ou la modification ou la suppression de règles existantes ne devrait pas avoir d'incidence sur le *débit ϕ_P de traitement des paquets* DPI nominal (avec ϕ_P égal à $\phi_{P,In}$).

8.2.3.3 Indicateur DPI "Taux d'erreurs"

Pour un nœud DPI, la somme du *taux de faux positifs* et du *taux de faux négatifs* donne le taux d'erreurs. Ces indicateurs de performance sont liés uniquement aux (éventuelles) décisions *statistiques* d'un nœud DPI. La fonction DPI-PEF aura un comportement déterministe pour la majorité des règles de politique DPI; toutefois, il pourrait y avoir des règles de politique DPI avec des conditions de politique statistiques ou des flux de paquets avec des informations de trafic statistiques qui peuvent conduire à des décisions incorrectes dans la fonction DPI-PEF.

Le Tableau 8-4 contient la définition de l'indicateur.

Tableau 8-4 – Indicateur DPI "taux d'erreurs"

Nom de l'indicateur:	N	Taux d'erreurs
Symbole:	I	ε_{DPI}
Description de l'indicateur:	N	La somme du taux de faux négatifs (voir le § 8.2.3.3.2) et du taux de faux positifs (voir le § 8.2.3.3.1) pour le nœud DPI.
Méthode de mesure ou de calcul:	N	Mesure directe: impossible (NOTE 2) Mesure indirecte (calcul): $\varepsilon_{DPI} = \varepsilon_{f-n} + \varepsilon_{f-p}$
Unité de mesure:	N	–
Point(s) de mesure avec domaine de mesure potentiel:	N	Voir la Figure 8-1 (modèle de trafic).
Intervalle de mesure:	N	L'intervalle de mesure dépend de l'échelle de temps du point de vue de l'instance d'utilisateur desservie. (NOTE 3)
Mise en œuvre:	I	–
Vérification:	I	–
Utilisation et applications:	I	"DPI en temps réel"
Modèle de notification:	I	Généralement dans le cadre de la gestion de la performance
Type "KPI": oui/non?	I	"KPI"
NOTE 1 – N: élément de description normatif; I: élément de description informatif. NOTE 2 – Cet indicateur de performance est ce que l'on appelle un indicateur *composé*; autrement dit, il ne peut pas être mesuré directement, mais résulte d'indicateurs *de base* qui ont été mesurés (voir le § 5.3.1 de [b-IETF RFC 6390]). NOTE 3 – L'instance d'utilisateur desservie représente en général une entité distante ("l'utilisateur"), intéressée par les mesures. Exemples: système de gestion de la performance, DPI PD-FE.		

8.2.3.3.1 Indicateur DPI "Taux de faux positifs"

Le Tableau 8-5 contient la définition de l'indicateur.

Tableau 8-5 – Indicateur DPI "Taux de faux positifs"

Nom de l'indicateur:	N	Taux de faux positifs
Symbole:	I	$\varepsilon_{f\text{-}p}$
Description de l'indicateur:	N	La proportion d'instances négatives signalées à tort comme étant positives.
Méthode de mesure ou de calcul:	N	La mesure de cet indicateur est très difficile; par conséquent, seules des indications peuvent être données dans la présente Recommandation: En général, un échantillon bien connu d'une série de paquets suffisamment vaste est envoyé à l'entité DPI. Le résultat *attendu* (donné par l'application des règles de politique DPI) est comparé aux résultats *mesurés* à partir du processus DPI. La mesure peut être effectuée dans le cadre de tests intrusifs ou non intrusifs.
Unité de mesure:	N	–
Point(s) de mesure avec domaine de mesure potentiel:	N	Voir la Figure 8-1 (modèle de trafic).
Intervalle de mesure:	N	L'intervalle de mesure dépend de l'échelle de temps du point de vue de l'instance d'utilisateur desservie.
Mise en œuvre:	I	–
Vérification:	I	–
Utilisation et applications:	I	"DPI en temps réel"
Modèle de notification:	I	Généralement dans le cadre de la gestion de la performance
Type "KPI": oui/non?	I	Oui
NOTE – N: élément de description normatif; I: élément de description informatif.		

Exemple 1:

Une condition de politique DPI C_i vise à identifier le "type d'application *X*" et la fonction d'identification des paquets (DPI-PIF) a donné comme résultat "type d'application *X*" pour un paquet de "type d'application *Y*", ce qui constitue un faux positif.

Exemple 2:

Le calcul de cet indicateur est possible pour l'inspection DPI probabiliste basée sur un filtre de Bloom (voir l'Appendice I) avec les paramètres suivants:

- m = taille du filtre de Bloom en bits
- n = nombre de signatures dans l'ensemble S
- k = nombre de fonctions de hachage utilisées pour la génération du filtre de Bloom

Le taux de faux positifs, $\varepsilon_{f\text{-}p}$, est donné par la formule:

$$\varepsilon_{f-p} = \left(1 - e^{-kn/m}\right)^k$$

Le résultat calculé et le résultat attendu peuvent ensuite être vérifiés par des mesures.

8.2.3.3.2 Indicateur DPI "Taux de faux négatifs"

Le Tableau 8-6 contient la définition de l'indicateur.

Tableau 8-6 – Indicateur DPI "Taux de faux négatifs"

Nom de l'indicateur:	N	Taux de faux négatifs
Symbole:	I	$\varepsilon_{f\text{-}n}$
Description de l'indicateur:	N	La proportion d'instances positives signalées à tort comme étant négatives.
Méthode de mesure ou de calcul:	N	Voir l'entrée correspondante dans le Tableau 8-5.
Unité de mesure:	N	–
Point(s) de mesure avec domaine de mesure potentiel:	N	Voir la Figure 8-1 (modèle de trafic)
Intervalle de mesure:	N	L'intervalle de mesure dépend de l'échelle de temps du point de vue de l'instance d'utilisateur desservie.
Mise en œuvre:	I	–
Vérification:	I	–
Utilisation et applications:	I	"DPI en temps réel"
Modèle de notification:	I	Généralement dans le cadre de la gestion de la performance
Type "KPI": oui/non?	I	Oui
NOTE – N: élément de description normatif; I: élément de description informatif.		

Exemple:

> Une condition de politique DPI C_i vise à identifier le "type d'application *X*" et la fonction d'identification des paquets (DPI-PIF) n'identifie pas un paquet de "type d'application *X*" comme étant de "type d'application *X*", ce qui constitue un faux négatif.

8.2.3.3.3 Relation avec les erreurs d'exécution

Le moteur DPI en tant qu'environnement d'exécution des règles de politique DPI est intrinsèquement non exempt d'erreur. Toutefois, le taux d'erreurs d'exécution et l'indicateur DPI "taux d'erreurs" représentent des indicateurs de performance différents.

Informations générales:

A titre d'exemple, la définition au § 4.1 de [b-IETF RFC 4011] de l'événement d'anomalie d'exécution donne des informations sur le concept d'erreurs d'exécution:

> "[…] anomalie d'exécution (RTE) – Une anomalie d'exécution est une erreur fatale causée dans le traitement d'un langage ou d'une fonction. Si, lors de l'invocation d'un script, une anomalie d'exécution se produit, il est immédiatement mis fin à l'exécution de ce script. En cas d'anomalie d'exécution pour une condition de politique lors du traitement d'un élément, l'élément ne sera pas considéré comme concordant à la condition et l'action associée ne sera pas exécutée sur cet élément. […]"

8.2.3.4 Indicateur DPI "Débit des paquets identifiés avec succès"

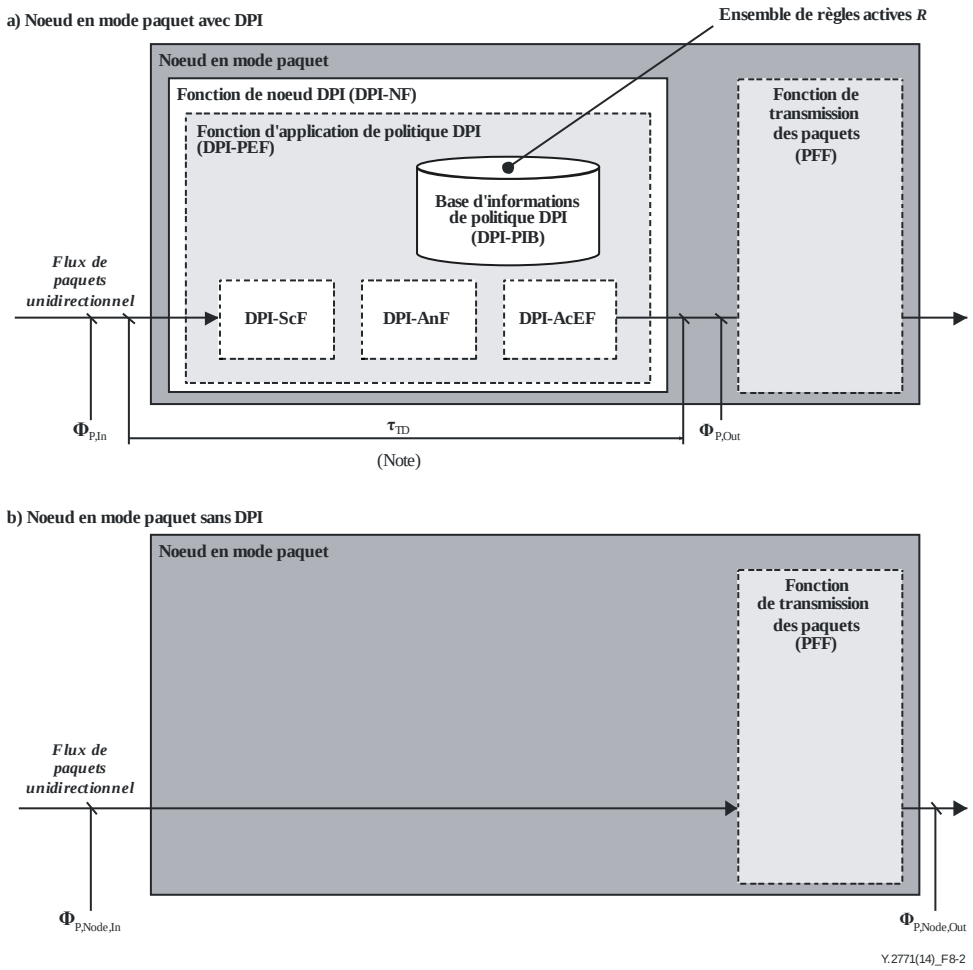
Le Tableau 8-7 contient la définition de l'indicateur.

Tableau 8-7 – Indicateur DPI "Débit des paquets identifiés avec succès"

Nom de l'indicateur:	N	Débit des paquets identifiés avec succès
Symbole:	I	$\phi_{P,Identified}$
Description de l'indicateur:	N	Un paquet entrant est "identifié avec succès" (par la fonction d'identification des paquets) lorsque les conditions de règle de politique DPI (pour au moins une règle de politique DPI) "concordent" pour le paquet inspecté. Le type de "concordance" (complète, partielle, déterministe, avec la probabilité …, etc.) n'est pas précisé plus avant. Le "débit" se rapporte au nombre de paquets identifiés avec succès par unité de temps.
Méthode de mesure ou de calcul:	N	1) Mesure directe: Par exemple: application d'une règle de politique DPI connue et génération d'un flux de paquets ayant des caractéristiques connues (autrement dit la part du trafic qui devrait concorder (ou non) est connue à l'avance). La valeur mesurée est ensuite comparée à la valeur nominale. 2) Mesure indirecte (calcul): $\phi_{P,Identified} = \phi_{P,In} \cdot (1 - \varepsilon_{DPI})$
Unité de mesure:	N	s^{-1}
Point(s) de mesure avec domaine de mesure potentiel:	N	Voir la Figure 8-1 (modèle de trafic).
Intervalle de mesure:	N	L'intervalle de mesure dépend de l'échelle de temps du point de vue de l'instance d'utilisateur desservie.
Mise en œuvre:	I	–
Vérification:	I	Voir la méthode ci-dessus "mesure directe".
Utilisation et applications:	I	"DPI en temps réel"
Modèle de notification:	I	Généralement dans le cadre de la gestion de la performance
Type "KPI": oui/non?	I	"KPI"
NOTE – N: élément de description normatif; I: élément de description informatif.		

8.3 Performance des points d'application de la politique, estimation du comportement qualitatif en termes de performance

Le présent paragraphe a pour objet de fournir des informations complémentaires concernant les estimations qualitatives de la performance pour l'application de politique en fonction de la couche de protocole. La Figure 8-2 illustre un nœud en mode paquet (a) avec une fonction de nœud DPI et (b) sans aucune inspection DPI appliquée. L'indicateur fondamental de performance considéré ici est le débit du nœud en mode paquet $\phi_{P,Node,Out}$.



NOTE – Le nœud en mode paquet et la fonction PFF apparaissent afin de spécifier sans ambiguïté les indicateurs de performance, mais les deux entités en tant que telles n'entrent pas dans le cadre de la présente Recommandation.

Figure 8-2 – Performance de l'application de la politique – Débit du nœud en mode paquet $\phi_{P,Node,Out}$ en fonction de l'ensemble de règles de politique appliquées $\underline{\underline{R}}$ à chaque paquet

La Figure 8-3 illustre les principales courbes de débit. Une fonction d'application de politique particulière (axe des y) est caractérisée par le nombre de règles de politique $\underline{\underline{R}}$ par paquet ainsi que par des aspects d'interaction entre les règles. L'application d'une règle de politique donnée consomme une certaine quantité de ressources du trajet des paquets en termes de temps de traitement, de mémoire des paquets, de mémoire TCAM/CAM, de base de données de politique, etc.

Règle empirique simplifiée: "plus il y a de règles pour chaque paquet, plus il faut de ressources pour appliquer la politique".

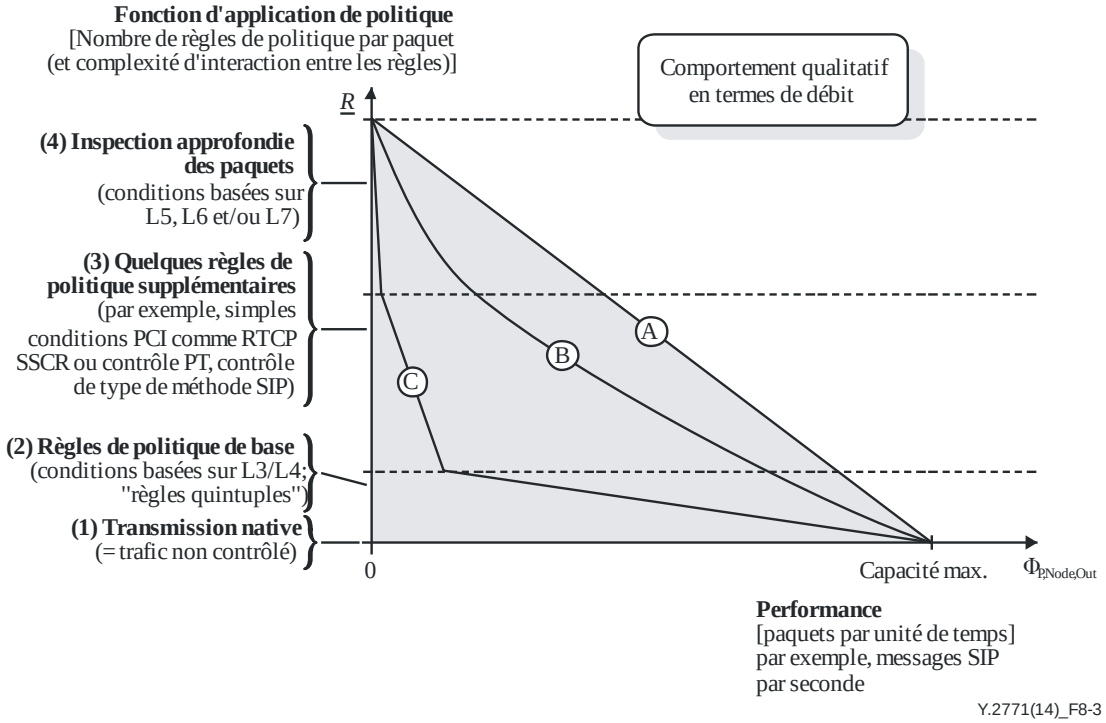


Figure 8-3 – Performance de l'application de la politique – Comportement qualitatif en termes de débit

Avec une mise en œuvre idéale, on obtiendrait un comportement "linéaire" de type *A*. Un modèle plus réaliste et présentant un bon rapport coût-efficacité serait plutôt celui de la courbe *C*.

La relation relativement *non-linéaire* du comportement *C* (voir la Figure 8-4) pose un problème technique (et commercial); il est en effet difficile de déterminer un point de charge nominal et/ou de parvenir au compromis nécessaire concernant la limitation de l'ensemble des règles de politique appliquées.

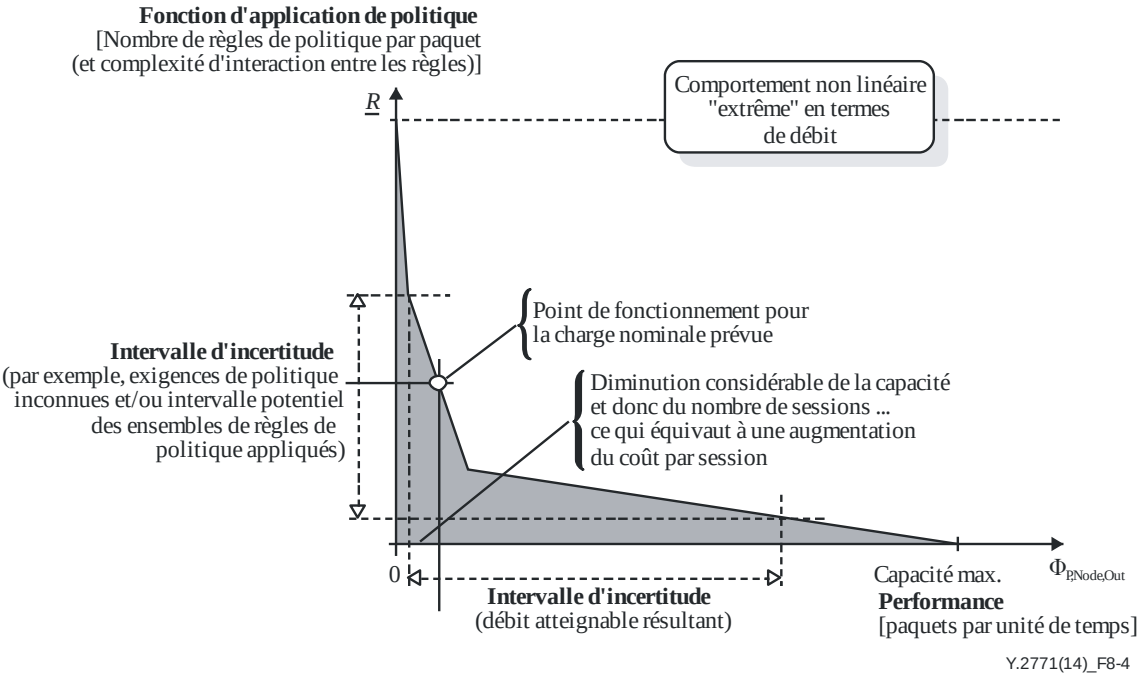


Figure 8-4 – Performance de l'application de la politique – Exemple de cas d'utilisation *C* en tant que scénario correspondant au cas le plus défavorable

9 Catégorisation des entités fonctionnelles DPI

En règle générale, une entité DPI ne prend pas en charge l'ensemble complet des exigences DPI énoncées dans la Recommandation [UIT-T Y.2770], mais simplement un sous-ensemble correspondant aux cas d'utilisation visés. Différents types d'entités DPI-FE pourraient par conséquent être identifiés.

9.1 Principes de catégorisation

Chaque capacité identifiable d'une entité DPI pourrait être associée à une ou plusieurs exigences DPI telles que spécifiées dans la Recommandation [UIT-T Y.2770]. Les capacités de haut niveau sont:

- les capacités en termes de traitement des conditions;
- les capacités en termes de traitement des actions; et
- éventuellement d'autres capacités.

Les critères types pour l'identification des types particuliers d'entité DPI-FE sont les scénarios de déploiement (cas d'utilisation DPI), la complexité de la logique de traitement, les facteurs de coût, etc.

9.2 Capacités en termes de traitement des conditions

Pour les capacités de traitement des conditions, on distingue deux catégories: L4 PI (prise en charge de l'inspection des données utiles L4) et non-L4 PI (absence de prise en charge de l'inspection des données utiles).

9.3 Capacités en termes de traitement des actions

Voir le § 6.3.3.1 de la Recommandation [UIT-T Y.2770] concernant les niveaux hiérarchiques des actions et des exemples.

9.4 Types d'entité DPI-FE

S'appuyant sur les principes de classification des § 9.2 et 9.3, le Tableau 9-1 donne un aperçu concernant trois types:

Tableau 9-1 – Types d'entité DPI-FE

<table>
<tr><th colspan="3" rowspan="3">Type d'entité DPI-FE</th><th colspan="2">Capacités en termes de traitement des actions</th></tr>
<tr><th colspan="2">Prise en charge de la fonction DPI-AcEF</th></tr>
<tr><th>Non</th><th>Oui</th></tr>
<tr><td rowspan="2">Capacités en termes de traitement des conditions</td><td rowspan="2">Prise en charge de l'inspection des données utiles L4</td><td>Non</td><td colspan="2">Type 1</td></tr>
<tr><td>Oui</td><td>Type 2</td><td>Type 3</td></tr>
</table>

En fonction des capacités fonctionnelles DPI d'une entité DPI-FE, on distingue les types suivants (Tableau 9-2):

Tableau 9-2 – Les trois types en détail

Type	Traitement des règles
1	Entité fonctionnelle ne prenant pas en charge l'inspection des données utiles L4 ($L_4PI = L_{4+}HI \cup L_7PI$), autrement dit une entité fonctionnelle non-DPI (par exemple une entité SPI-FE)
2	Entité DPI-FE ne prenant pas en charge l'exécution des actions (DPI-AcFE), mais prenant en charge l'inspection des données utiles L4 ($L_4PI = L_{4+}HI \cup L_7PI$)
3	Entité DPI-FE prenant en charge l'exécution des actions (DPI-AcFE) ainsi que l'inspection des données utiles L4 ($L_4PI = L_{4+}HI \cup L_7PI$)

Le type d'une entité DPI-FE pourrait dépendre de facteurs tels que:

1) la quantité de ressources disponibles: capacités d'une entité physique DPI particulière (DPI-PE) (comme les composants matériels (HW) ou logiciels (SW)); ou

2) la quantité de ressources attribuées/activées pour le traitement DPI: via la gestion de la configuration (par exemple via les entités de gestion de la politique (voir le § 7) par la fourniture d'un ensemble de capacités particulier).

Il est à noter qu'une entité DPI-FE particulière de type *n* peut être configurée comme étant de type *m* (n > m) par son entité de gestion (du fait que, par exemple, l'"ensemble de capacités DPI pour le type 3" est un superensemble par rapport aux autres types).

Une entité DPI-FE devrait pouvoir signaler son type aux entités fonctionnelles connexes (par exemple la fonction RACF).

En fonction des capacités fonctionnelles DPI d'une entité DPI-FE de type 3, on distingue les sous-variantes suivantes (Tableau 9-3):

Tableau 9-3 – Sous-variantes du type 3

Type	Traitement des règles
3.1	Entité DPI-FE prenant en charge la collecte et la notification d'informations
3.2	Type 3.1 avec la prise en charge de la commande du trafic, mais sans la prise en charge de la modification du contenu des paquets
3.3	Type 3.2 avec la prise en charge de la modification du contenu des paquets

10 Considérations relatives à la sécurité

Les aspects liés à la réglementation, à la confidentialité et à la sécurité des applications DPI n'entrent pas dans le cadre de la présente Recommandation. Les fabricants, opérateurs et fournisseurs de service doivent tenir compte de la réglementation et des politiques nationales lorsqu'ils appliquent la présente Recommandation.

Conformément à la Recommandation [UIT-T Y.2770], l'entité DPI-FE et les informations concernant les opérations DPI devraient être protégées contre les menaces. Les mécanismes spécifiés dans la Recommandation [UIT-T Y.2704] répondent aux exigences de sécurité énoncées dans la Recommandation [UIT-T Y.2770].

Appendice I

Exemple d'architecture fonctionnelle de l'inspection DPI probabiliste basée sur un filtre de Bloom

(Cet appendice ne fait pas partie intégrante de la présente Recommandation.)

I.1 Introduction

Le filtre de Bloom est décrit dans la référence [b-Bloomfilter]:

Les filtres de Bloom utilisent une technique randomisée pour déterminer l'appartenance à un ensemble de chaînes. Pour une chaîne donnée, le filtre de Bloom lui applique *k* fonctions de hachage produisant des empreintes comprises entre de 1 et *m* (voir la Figure I-1). Ensuite, il met à 1 les *k* bits d'un vecteur de m bits situés aux positions correspondant aux *k* empreintes, où *k* n'est pas supérieur à *m* (voir aussi la formule [7-1]). La même procédure est répétée pour tous les membres de l'ensemble. Ce processus est appelé "programmation" du filtre. Le processus de requête est analogue au processus de programmation. Une chaîne dont on souhaite vérifier si elle appartient à l'ensemble est introduite dans le filtre de Bloom, lequel génère *k* empreintes en utilisant les mêmes fonctions de hachage que celles qu'il a utilisées pour programmer le filtre. On s'intéresse aux bits du vecteur de m bits situés aux positions correspondant aux *k* empreintes. Si au moins un de ces bits vaut 0, la chaîne est déclarée ne pas appartenir à l'ensemble. Si tous les bits valent 1, la chaîne est déclarée appartenir à l'ensemble avec une certaine probabilité. Cette incertitude quant à l'appartenance vient du fait que ces *k* bits présents dans le vecteur de m bits peuvent être mis à 1 par n'importe lequel des membres. Par conséquent, la présence d'un bit valant 1 n'implique pas nécessairement qu'il a été mis à 1 par la chaîne particulière sur laquelle porte la requête. Toutefois, la présence d'un bit valant 0 implique avec certitude que la chaîne n'appartient pas à l'ensemble, car, si elle appartenait à l'ensemble, les *k* bits auraient avec certitude été mis à 1 lors de la programmation du filtre de Bloom avec cette chaîne. C'est pourquoi il peut y avoir des faux positifs, mais il ne peut y avoir de faux négatifs.

A titre d'exemple, dans la Figure I.1, le filtre de Bloom BF (B[0..m-1]) est généré par 3 fonctions de hachage, h1, h2 et h3, sur les chaînes x1 et x2; pour l'inspection DPI basée sur ce filtre, les chaînes x1 et x2 sont les signatures DPI. Les chaînes y1 et y2 sont vérifiées moyennant l'application à ces chaînes des 3 fonctions de hachage h1, h2 et h3 du filtre de Bloom BF (donné par le vecteur B[0..m-1]); pour l'inspection DPI basée sur ce filtre, les chaînes y1 et y2 représentent les structures de données inspectées, correspondant par exemple aux données utiles des paquets entrants.

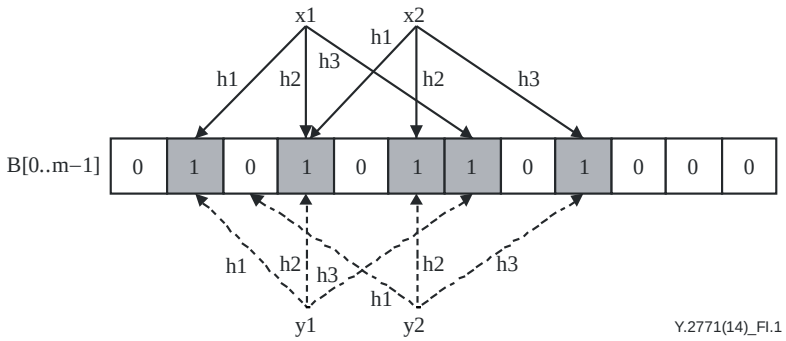


Figure I.1 – Programmation d'un filtre de Bloom (correspondant au vecteur B[0..m-1]) et requête

Le taux de faux positifs, ε_{f-p}, est donné par la formule I-1:

$$\varepsilon_{f-p} = \left(1 - e^{-kn/m}\right)^k \quad \text{(I-1)}$$

où *n* est le nombre de chaînes programmées dans le filtre de Bloom. On peut diminuer la valeur de ε_{f-p} en choisissant des valeurs appropriées de *m* et *k* pour un nombre donné de membres dans l'ensemble, *n*.

I.2 Modèle fonctionnel de l'inspection DPI probabiliste basée sur un filtre de Bloom

Le modèle fonctionnel de l'inspection DPI probabiliste basée sur un filtre de Bloom est illustré dans la Figure I-2. La règle de politique pour l'inspection DPI probabiliste peut être la suivante:

Si le paquet 'P' contient des signatures d'un ensemble de signatures DPI '*S'* (condition de politique), où l'ensemble de signatures est donné par '*S'={'S1',' S2',..., 'Sm'}*, alors éliminer le paquet (action de politique).

Le filtre de Bloom BF_S pour l'ensemble de signatures S est généré par l'ensemble de fonctions de hachage H_1, H_2, …, H_k. La règle de politique devient:

Si H_1('P'), H_2('P'), …, H_k('P') concorde avec BF_S, alors éliminer le paquet.

Avant que l'analyseur DPI compare le paquet arrivant avec cette condition de règle de politique DPI, le scanner DPI doit déterminer le décalage et la longueur pour le paquet arrivant à utiliser pour la comparaison.

Il existe deux possibilités principales:

1) Pour une condition de règle DPI dépendante de la pile de protocoles, le décalage et la longueur de la signature dans l'ensemble 'S' sont connus, et le scanner communique directement à l'analyseur DPI les informations de décalage et de longueur.

2) Pour une condition de règle DPI indépendante du protocole, le scanner DPI doit effectuer un balayage pour déterminer le décalage et la longueur. Il communique ensuite ces informations à l'analyseur DPI.

L'analyseur DPI génère le résultat de hachage du paquet P à l'aide de H_1, H_2, …, H_k, le compare à BF_S et communique le résultat de concordance à la fonction d'exécution d'action DPI. La fonction d'exécution d'action DPI communique le résultat de concordance ("vrai" ou "faux"). Si ce résultat est estimé comme ayant la valeur "vrai", elle élimine le paquet; dans le cas contraire, elle transmet le paquet à la fonction de transmission des paquets. Si le résultat de concordance généré ne correspond pas à BF_s, le scanner DPI doit effectuer un balayage à partir de l'octet "décalage+1" (décalage = décalage + 1), et ainsi de suite jusqu'à la fin du paquet.

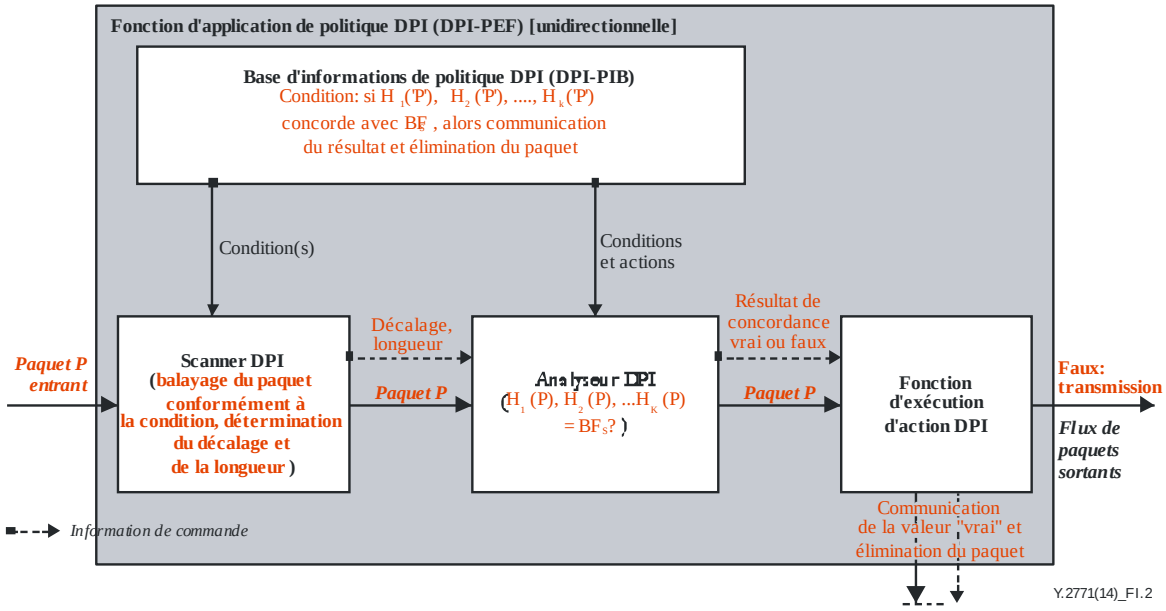


Figure I.2 – Modèle fonctionnel de l'inspection DPI probabiliste basée sur un filtre de Bloom

On notera que le résultat de concordance donné par l'analyseur DPI est de type booléen, à savoir vrai ou faux, et ne fournit aucune valeur de probabilité, par exemple "*concordance positive avec la probabilité* ***p*** (p compris entre 0% et 100%)". Toutefois, le trajet de traitement des paquets DPI complet conduit à des résultats DPI probabilistes en raison du taux de faux positifs, $\varepsilon_{f\text{-}p}$, inhérent à la condition de politique DPI.

Bibliographie

[b-UIT-T H.248.53] Recommandation UIT-T H.248.53 (2009), *Protocole de commande de passerelle: Paquetages de gestion du trafic*.

[b-UIT-T I.130] Recommandation UIT-T I.130 (1988), *Méthode de caractérisation des services de télécommunication assurés sur un RNIS et des possibilités réseau d'un RNIS*.

[b-UIT-T J.380.1] Recommandation UIT-T J.380.1 (2011), *Insertion de programmes numériques – Interfaces avec les systèmes de publicité – Aperçu des systèmes de publicité*.

[b-UIT-T X.1036] Recommandation UIT-T X.1036 (2007), *Cadre applicable à la création, au stockage, à la distribution et à la mise en vigueur des politiques de sécurité de réseau*.

[b-UIT-T Y.1221] Recommandation UIT-T Y.1221 (2010), *Gestion du trafic et des encombrements dans les réseaux en mode IP*.

[b-UIT-T Y.2121] Recommandation UIT-T Y.2121 (2008), *Spécifications applicables à la prise en charge d'une technique de transport fondée sur l'état des flux dans un NGN*.

[b-UIT-T Y-Sup.23] Recommandations UIT-T de la série Y – Supplément 23 (2013), série UIT-T Y.2770 – *Supplément sur la terminologie relative à l'inspection approfondie des paquets*.

[b-IETF RFC 1812] IETF RFC 1812 (1995), *Requirements for IP Version 4 Routers*.

[b-IETF RFC 2544] IETF RFC 2544 (1999), *Benchmarking Methodology for Network Interconnect Devices*.

[b-IETF RFC 3060] IETF RFC 3060 (2001), *Policy Core Information Model – Version 1 Specification*.

[b-IETF RFC 3198] IETF RFC 3198 (2001), *Terminology for Policy-Based Management*.

[b-IETF RFC 4011] IETF RFC 4011 (2005), *Policy Based Management MIB.*

[b-IETF RFC 4292] IETF RFC 4292 (2006), *IP Forwarding Table MIB.*

[b-IETF RFC 6390] IETF RFC 6390 (2011), *Guidelines for Considering New Performance Metric Development*.

[b-Bloomfilter] Dharmapurikar, S. et al., (2003), *Implementation of a Deep Packet Inspection Circuit using Parallel Bloom Filters in Reconfigurable Hardware. IEEE Proceedings of 11th Symposium on High Performance Interconnects. Stanford University, Wiley, John & Sons, Inc*.

[b-CRTC] *Conseil de la radiodiffusion et des télécommunications canadiennes (2009), Technologies de gestion du trafic des FSI: Etat des connaissances*.

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

Imprimé en Suisse
Genève, 2015