الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

Y.2770

(2012/11)

السلسلة Y: البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي

شبكات الجيل التالي – الأمن

متطلبات التفتيش المتعمق على الرزمة في شبكات الجيل التالي

التوصيـــة ITU-T Y.2770

الاتحاد الدولي للاتصالات

توصيات السلسلة Y الصادرة عن قطاع تقييس الاتصالات

البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي

البنية التحتية العالمية للمعلومات	
اعتبارات عامة	Y.199-Y.100
الخدمات والتطبيقات، والبرمجيات الوسيطة	Y.299-Y.200
الجوانب الخاصة بالشبكات	Y.399-Y.300
السطوح البينية والبروتوكولات	Y.499-Y.400
الترقيم والعنونة والتسمية	Y.599-Y.500
الإدارة والتشغيل والصيانة	Y.699-Y.600
الأمن	Y.799-Y.700
مستويات الأداء	Y.899-Y.800
جوانب متعلقة ببروتوكول الإنترنت	
اعتبارات عامة	Y.1099-Y.1000
الخدمات والتطبيقات	Y.1199-Y.1100
المعمارية والنفاذ وقدرات الشبكة وإدارة الموارد	Y.1299-Y.1200
النقل	Y.1399-Y.1300
التشغيل البيني	Y.1499-Y.1400
نوعية الخدمة وأداء الشبكة	Y.1599-Y.1500
التشوير	Y.1699-Y.1600
الإدارة والتشغيل والصيانة	Y.1799-Y.1700
الترسيم	Y.1899-Y.1800
تلفزيون بروتوكول الإنترنت عبر شبكات الجيل التالي	Y.1999-Y.1900
شبكات الجيل التالي	
الإطار العام والنماذج المعمارية الوظيفية	Y.2099-Y.2000
نوعية الخدمة والأداء	Y.2199-Y.2100
الجوانب الخاصة بالخدمة: قدرات ومعمارية الخدمات	Y.2249-Y.2200
الجوانب الخاصة بالخدمة: إمكانية التشغيل البيني للخدمات والشبكات	Y.2299-Y.2250
الترقيم والتسمية والعنونة	Y.2399-Y.2300
إدارة الشبكة	Y.2499-Y.2400
معمارية الشبكة وبروتوكولات التحكم في الشبكة	Y.2599-Y.2500
الشبكات الذكية الشمولية	Y.2699-Y.2600
الأمن	**Y.2799-Y.2700**
التنقلية المعممة	Y.2899-Y.2800
البيئة المفتوحة عالية الجودة	Y.2999-Y.2900
شبكات المستقبل	Y.3499-Y.3000
الحوسبة السحابية	Y.3999-Y.3500

لمزيد من التفاصيل، يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصيـــة ITU-T Y.2770

متطلبات التفتيش المتعمق على الرزمة في شبكات الجيل التالي

ملخص

توصّف التوصية ITU-T Y.2770 متطلبات التفتيش المتعمق على الرزمة (DPI) في شبكات الجيل التالي (NGN). وتوصّف هذه التوصية في المقام الأول متطلبات كيانات التفتيش المتعمق على الرزمة (DPI) في شبكات الجيل التالي متناولةً، على وجه الخصوص، جوانب مثل تحديد هوية التطبيق وتحديد هوية التدفق وأنماط الحركة الخاضعة للتفتيش وإدارة التوقيع وإبلاغ نظام إدارة الشبكة (NMS) والتفاعل مع الكيان الوظيفي المعني بقرار السياسة المتبعة. ورغم أن هذه المتطلبات تستهدف شبكات الجيل التالي، فقد تكون قابلة للتطبيق على أنواع أخرى من الشبكات.

التسلسل التاريخي

الصيغة	التوصية	تاريخ الموافقة	لجنة الدراسات
1.0	ITU-T Y.2770	2012.11.20	13

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات وتكنولوجيات المعلومات والاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA) التي تجتمع مرة كل أربع سنوات المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظـــة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

جدول المحتويات

الصفحة

متطلبات التفتيش المتعمق على الرزمة في شبكات الجيل التالي

1 مجال التطبيق

توصّف هذه التوصية في المقام الأول متطلبات كيانات التفتيش المتعمق على الرزمة (DPI) في شبكات الجيل التالي متناولةً على وجه الخصوص جوانب مثل تحديد هوية التطبيق وتحديد هوية التدفق وأنماط الحركة الخاضعة للتفتيش وإدارة التوقيع وإبلاغ نظام إدارة الشبكة (NMS) والتفاعل مع الكيان الوظيفي المعني بقرار السياسة المتبعة.

كما تحدد هذه التوصية متطلبات التفتيش المتعمق على رزم (DPI) حركة أنساق التشفير غير المحلية (مثل الحركة المجفَّرة والبيانات المضغوطة والمعلومات المحولة الشفرة).

ويمكن بصفة عامة وصف أي وظيفة من وظائف التفتيش المتعمق على الرزمة (DPI) بمفهوم قواعد السياسة المتبعة (انظر الفقرة 2.1).

ويتعين على منفذي التقنيات الموصوفة ومستخدميها الامتثال لجميع القوانين واللوائح والسياسات الوطنية والإقليمية المعمول بها. ويجوز عدم تطبيق الآلية الموصوفة في هذه التوصية على المراسلات الدولية من أجل ضمان السرية والمتطلبات القانونية للسيادة الوطنية المفروضة على الاتصالات ودستور الاتحاد واتفاقيته.

ولا تتناول التوصية التأثير الخاص لتنفيذ الخواص الوظيفية الموزعة للتفتيش المتعمق على الرزمة (DPI).وتتصل المتطلبات في المقام الأول بالجوانب الوظيفية للتفتيش المتعمق على الرزمة، ولكن الجوانب المادية مشمولة أيضاً. وفي سياق سيناريوهات التقابل بين الكيانين الوظيفي والمادي، لا يشمل مجال تطبيق هذه التوصية إلا تقابل 1 إلى 1 وتقابل N إلى 1 بين كيان وظيفي للتفتيش المتعمق على الرزمة (DPI-FE) وكيان مادي للتفتيش المتعمق على الرزمة (DPI-PE). وبعبارة أخرى، لا توجد متطلبات تشمل الكيانات المادية الموزعة للتفتيش المتعمق على الرزمة.

1.1 السيناريوهات التي تسري عليها هذه التوصية

تسري هذه التوصية على السيناريوهات المحددة في الشكل 1-1:

		نمط الشبكة القائم على الرزم	
		NGN	غير NGN
تكنولوجيا حالة الرزم	IP	تسري عليه التوصية	ربما تسري عليه التوصية
	غير IP	ربما تسري عليه التوصية	ربما تسري عليه التوصية

Y.2770(12)_F1-1

الشكل 1-1 – السيناريوهات التي تسري عليها هذه التوصية

يشير مفهوم "غير بروتوكول الإنترنت" إلى كدسات بروتوكولية لأنماط حامل الكدسات الخالية من أي طبقة بروتوكول إنترنت ([IETF RFC 791] و[IETF RFC 2460]).

ورغم أن هذه التوصية تتناول أساساً متطلبات التفتيش المتعمق على الرزمة في شبكات الجيل التالي، فقد تنطبق هذه المتطلبات على أنواع أخرى من الشبكات، ويُترك هذا الأمر لمزيد من الدراسة.

2.1 قواعد السياسة المتبعة

تفترض هذه التوصية نسقاً عاماً رفيع المستوى لجميع قواعد السياسة المتبعة. ويسري هذا النسق على قواعد التفتيش المتعمق على الرزمة (DPI) على النحو المبين في الشكل 1-2. ويميز هذا النسق ثلاث كتل أساسية من:

'1' قواعد محدد الهوية/الاسم (مع بيان الرتبة/الترتيب نظراً لإمكانية تعدد القواعد)؛

'2' توقيع/شروط التفتيش المتعمق على الرزمة (DPI)؛

'3' الإجراءات.

وهناك إسناد منطقي بين الإجراء (الإجراءات) والشرط (الشروط)، انظر الفقرة 2.1.3.

الشكل 1-2 – النسق العام لقواعد السياسة المتبعة

لاحظ أن الجوانب التالية تقع في مجال تطبيق هذه التوصية:

- توصيف المتطلبات الخاصة بتوقيع التفتيش المتعمق على الرزمة (DPI)، (أي تواقيع DPI المستخدمة لتحديد هوية تطبيق وتحديد هوية تدفق)؛
- وتوصيف المتطلبات المتعلقة بتحديد قواعد سياسة التفتيش المتعمق على الرزمة (DPI) وتسميتها؛
- وتحديد السيناريوهات المحتملة التي تنطوي على إجراءات السياسة المتبعة وأنشطة المتابعة المحتملة بعد تقييم تواقيع DPI.

وفي المقابل، تقع الجوانب التالية خارج مجال تطبيق هذه التوصية:

- مواصفات المتطلبات المتعلقة بالإجراءات الخاصة بتعديل رزمة (أو رزم) خاضعة للتفتيش؛
- وتوصيف الأسانيد الصريحة بين الإجراءات والشروط (ملاحظة)؛
- وتوصيف قواعد سياسة التفتيش المتعمق على الرزمة (DPI) بالكامل؛
- وتوصيف لغة لتواقيع التفتيش المتعمق على الرزمة (DPI)؛
- مواصفات الشروط ذات المدلول لسياسة التفتيش المتعمق على الرزمة (DPI) (مثل الوظائف السلوكية أو الإحصائية).

ملاحظـــة – على سبيل المثال، قد يكون هناك توصيف لإجراء نبذ رزمة وشرط البحث عن توقيع رزمة، ولكن *لن* يكون هناك أي توصيف يقرن الإجراء الفردي بشرط فعلي.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، نحث جميع المستعملين لهذه التوصية على السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T E.107] التوصية ITU-T E.107 (2007)، *خدمات الاتصالات في حالة الطوارئ (ETS) وهيكل التوصيل البيني لعمليات التنفيذ الوطنية لهذه الخدمات.*

[ITU-T X.200] التوصية المعيار الدولي ISO/IEC 7498-1:1994 | ITU-T X.200 (1994)، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – النموذج المرجعي الأساسي: النموذج الأساسي.*

[ITU-T X.731] التوصية ITU-T X.731 (1992)، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – إدارة الأنظمة: وظيفة إدارة الحالات.*

[ITU-T Y.1221] التوصية ITU-T X.1221 (2010)، *التحكم في الحركة والازدحام في الشبكات القائمة على بروتوكول الإنترنت.*

[ITU-T Y.2111] التوصية ITU-T Y.2111 (2008)، *وظائف التحكم في الموارد والقبول في شبكات الجيل التالي.*

[ITU-T Y.2205] التوصية ITU-T Y. 2205 (2011)، *شبكات الجيل التالي – اتصالات الطوارئ – اعتبارات تقنية.*

[ITU-T Y.2701] التوصية ITU-T Y.2701 (2007)، *متطلبات الأمن بالنسبة إلى الإصدار الأول لشبكات الجيل التالي.*

[ITU-T Y.2704] التوصية ITU-T Y.2704 (2007)، *آليات وإجراءات الأمن لشبكات الجيل التالي.*

[IETF RFC 791] IETF RFC 791 (1981), *Internet Protocol*.

[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 التعاريف

1.3 مصطلحات معرَّفة في أماكن أخرى

تستعمل هذه التوصية المصطلحات التالية المعرفة في أماكن أخرى:

1.1.3 مرشاح [b-IETF RFC 3198]: مجموعة من المصطلحات و/أو المعايير المستخدمة لأغراض الفصل أو التصنيف. ويُنجز ذلك عن طريق مطابقة ميدان واحد أو ميادين متعددة لرأسية الحركة و/أو بيانات الحمولة. وكثيراً ما تُضبط "المراشيح" وتُستخدم في تشغيل الشبكات والسياسة الناظمة لها. فعلى سبيل المثال، توصّف مراشيح الرزم معايير لمطابقة نمط (مثل بروتوكول الإنترنت أو معايير 802) للتمييز بين أصناف الحركة القابلة للفرز.

ملاحظـــة – في هذه التوصية، يكون مصطلح "رأسية الحركة" مرادفاً "لرأسية الرزمة".

2.1.3 قاعدة المرشاح/السياسة المتبعة [b-IETF RFC 3198]: هي لبنة أساسية في نظام قائم على سياسة متبعة. وهي إسناد مجموعة من الإجراءات إلى مجموعة من الشروط، حيث تقيَّم الشروط لتحديد ما إذا كانت الإجراءات منفَّذة.

ملاحظـــة – في هذه التوصية، تكون قاعدة مرشاح قاعدة سياسة محددة تهدف لفصل الحركة، على سبيل المثال، في فئتي "مقبول" و"غير مقبول" الرئيسيتين.

3.1.3 تدفق [IETF RFC 5101]: مجموعة من رزم بروتوكول الإنترنت تعبر نقطة رصد في الشبكة خلال فترة زمنية معينة. ولكل الرزم المنتمية لتدفق معين مجموعة من الخصائص المشتركة. وتعرَّف كل خاصية نتيجة لتطبيق وظيفة على قيم ما يلي:

1) واحد أو أكثر من حقول رأسية الرزمة (مثل عنوان المقصد وفق بروتوكول الإنترنت) أو حقول رأسية (مثل رقم منفذ المقصد) أو حقول رأسية التطبيق (مثل حقول رأسية بروتوكول النقل في الوقت الفعلي (RTP) [b-IETF RFC 3550]).

2) واحدة أو أكثر من خصائص الرزمة نفسها (مثل عدد وسوم تبديل الوسوم بعدة بروتوكولات (MPLS)، إلخ).

3) واحد أو أكثر من الحقول المشتقة من معالجة الرزمة (عنوان القفزة التالية وفق بروتوكول الإنترنت، والسطح البيني للخرج).

وتُعرَّف رزمة على أنها تنتمي إلى تدفق إذا استوفت تماماً كل الخصائص المحددة للتدفق.

ويشمل هذا التعريف المدى الممتد من تدفق يحتوي على كل الرزم المرصودة في السطح البيني للشبكة إلى تدفق يتألف من رزمة واحدة فقط بين تطبيقين. ويتضمن الرزم التي اختارتها آلية أخذ العينات.

ملاحظـــة – تبين البنود المرقمة المدرجة أعلاه خصائص التدفق في فئات (1) "معلومات التحكم في بروتوكول (PCI) الرزم"، و(2) "خصائص وحدة بيانات بروتوكول (PDU) الرزم" و(3) "معلومات إعادة توجيه الرزمة المحلية".

4.1.3 السياسة المتبعة [b-IETF RFC 3198]: مجموعة من القواعد لإدارة موارد الشبكة والتصرف بها والتحكم في النفاذ إليها.

2.3 المصطلحات المعرّفة في هذه التوصية

تعرّف هذه التوصية المصطلحات التالية:

1.2.3 التطبيق: يشير إلى إحدى الدلالات التالية:

- *نمط بروتوكول التطبيق* (مثل بروتوكولات تطبيق بروتوكول الإنترنت أو الفيديو وفق معيار التوصية ITU-T H.264 أو بروتوكول استهلال الدورة (SIP))؛
- *مثال مستخدم مخدَّم* (بالصوت عبر بروتوكول الإنترنت (VoIP) أو الصوت عبر معيار التطور في المدى البعيد (VoLTE) أو الصوت عبر خدمة تعدد وسائط بروتوكول الإنترنت (VoIMS) أو الصوت عبر شبكات الجيل التالي (VoNGN) والصوت عبر الربط الشبكي بين النظراء (VoP2P) مثلاً) في أحد أنماط التطبيق مثل "تطبيق الصوت عبر الرزمة"؛
- "*تطبيق مخصص لمورّد معين*" في الصوت عبر الرزمة (مثل VoIP لمورّد 3GPP وSkype VoIP)؛
- تطبيق مدمج في تطبيق آخر (مثل محتوى تطبيق في عنصر في متن بروتوكول استهلال الدورة (SIP) أو رسالة HTTP).

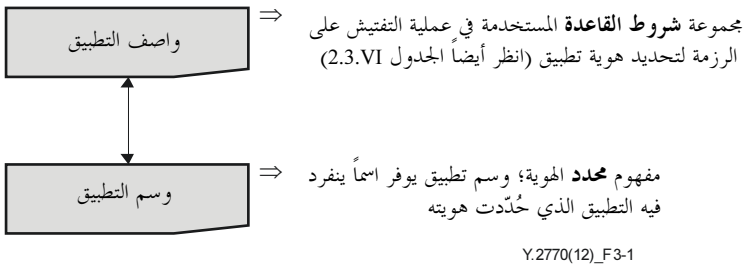
ويُتعرَّف على تطبيق بمحدد هوية معين (مثل حقل بتات أو نمط أو توقيع أو تعبير عادي من قبيل "شروط مستوى التطبيق"، انظر أيضاً الفقرة 2.2.3)، وهذه خاصية مشتركة من جميع المستويات المذكورة أعلاه من التطبيقات.

2.2.3 واصف التطبيق (المعروف أيضاً باسم شروط مستوى التطبيق): مجموعة من شروط القاعدة التي تحدد التطبيق (وفقاً للفقرة 1.2.3).

وتتناول هذه التوصية واصف التطبيق ككائن، بوجه عام، يرادف شروط مستوى التطبيق. فلا تتعمق في تفاصيل هيكلة مثل قواعد التركيب اللغوي فيه وتشفيره ونمط بياناته.

3.2.3 وسم التطبيق: اسم ينفرد به التطبيق ويُستخدم لبيان مدلولاته وعادة ما يستخدم في سيناريوهات الإبلاغ.

ويوضح الشكل 3-1 العلاقة بين سمة التطبيق وواصف التطبيق.



الشكل 3-1 – العلاقة بين سمة التطبيق وواصف التطبيق

4.2.3 التفتيش المتعمق على الرزمة (DPI) ثنائي الاتجاه: تفتيش متعمق على الرزمة يتضمن شروط السياسة المتبعة بشأن الحركة في كلا الاتجاهين.

ملاحظـــة – هناك ما لا يقل عن شرط بسيط واحد لكل اتجاه حركة في حالة التفتيش المتعمق على الرزمة ثنائي الاتجاه.

5.2.3 التفتيش المتعمق على الرزمة (DPI): تحليل، وفق معمارية البروتوكول ذات الطبقات في النموذج المرجعي الأساسي للتوصيل البيني للأنظمة المفتوحة (OSI-BRM) [ITU-T X.200]، لما يلي:

- خصائص الحمولة و/أو الرزمة (انظر قائمة الخصائص المحتملة في الفقرة 11.2.3) ومعلومات الرأسية في الطبقات الأعمق من الطبقات البروتوكولية 2 أو 3 أو 4 (L2/L3/L4)،
- وخصائص الرزمة الأخرى

وذلك من أجل تحديد هوية التطبيق على نحو لا لبس فيه.

ملاحظـــة – عادة ما يُستخدم خرج وظيفة التفتيش المتعمق على الرزمة (DPI) إلى جانب بعض المعلومات الإضافية، مثل تدفق المعلومات، في وظائف لاحقة مثل التقارير المقدمة أو الإجراءات بشأن الرزمة.

6.2.3 محرك التفتيش المتعمق على الرزمة (DPI): هو جزء مكون ومركزي من الكيان الوظيفي للتفتيش المتعمق على الرزمة الذي يقوم بجميع وظائف المعالجة في مسير الرزمة (على سبيل المثال، تحديد هوية الرزمة وغيرها من وظائف معالجة الرزمة في الشكل 6-1).

7.2.3 كيان التفتيش المتعمق على الرزمة (DPI): كيان التفتيش المتعمق على الرزمة هو إما كيان وظيفي أو كيان مادي للتفتيش المتعمق على الرزمة.

8.2.3 الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE): كيان وظيفي ينفذ التفتيش المتعمق على الرزمة.

9.2.3 الكيان المادي للتفتيش المتعمق على الرزمة (DPI-PE): مثال منفَّذ من الكيان الوظيفي للتفتيش المتعمق على الرزمة.

10.2.3 سياسة التفتيش المتعمق على الرزمة (DPI): سياسة على النحو المحدد في المعيار [b-IETF RFC 3198] مثلاً (انظر الفقرة 4.1.3) يجري إنفاذها في كيان تفتيش متعمق على الرزمة.

11.2.3 شرط سياسة التفتيش المتعمق على الرزمة (DPI) (المعروف أيضاً باسم توقيع التفتيش المتعمق على الرزمة): تمثيل للحالة اللازمة و/أو المقتضيات المسبقة التي تحدد هوية تطبيق وتحدد ما إذا كان ينبغي تنفيذ إجراءات قاعدة السياسة المتبعة. وتحدد مجموعة شروط سياسة التفتيش المتعمق على الرزمة المرتبطة بقاعدة السياسة المتبعة متى تسري هذه القاعدة (انظر أيضاً [b-IETF RFC 3198]).

ويجب أن يتضمن شرط سياسة التفتيش المتعمق على الرزمة (DPI) شروط مستوى التطبيق وقد يشمل خيارات أخرى مثل شروط الحالة و/أو شروط مستوى التدفق:

1) شرط الحالة (اختياري):

أ) شروط درجة الخدمة في الشبكة (على سبيل المثال، الازدحام الملموس في مسيرات الرزمة)؛ أو

ب) حالة عناصر الشبكة (على سبيل المثال، شرط الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) بشأن الحمل الزائد محلياً).

2) واصف التدفق/شروط مستوى التدفق (اختياري):

أ) محتوى الرزمة (حقول الرأسية)؛

ب) خصائص رزمة (مثل رقم (#) وسوم MPLS)؛

ج) معالجة الرزمة (على سبيل المثال، السطح البيني لخرج الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE).

3) واصف التطبيق/شروط مستوى التطبيق:

أ) محتوى الرزمة (حقول رأسية التطبيق وحمولة التطبيق).

ملاحظـــة – يتعلق الشرط "بالشرط البسيط" في الأوصاف الرسمية لشروط مستوى التدفق وشروط مستوى التطبيق.

12.2.3 الكيان الوظيفي المعني بقرار سياسة التفتيش المتعمق على الرزمة (DPI-PDFE): الوظيفة البعيدة عن الكيان (DPI-FE) التي تقرر أي من القواعد القائمة على التوقيع سيجري إنفاذها في الكيان DPI-FE. وقد لا تبتعد بعض وظائف التحكم و/أو الإدارة بالضرورة عن DPI-FE.

13.2.3 قاعدة سياسة التفتيش المتعمق على الرزمة (DPI): قاعدة السياسة المعنية بالتفتيش المتعمق على الرزمة (انظر أيضاً الفقرة 2.1.3). وفي هذه التوصية، يشار إلى قاعدة سياسة التفتيش المتعمق على الرزمة بمجرد "قاعدة".

14.2.3 توقيع التفتيش المتعمق على الرزمة (DPI): مرادف شرط (أو شروط) سياسة التفتيش المتعمق على الرزمة (DPI) (انظر الفقرة 11.2.3).

15.2.3 مكتبة تواقيع التفتيش المتعمق على الرزمة (DPI): قاعدة بيانات تتألف من مجموعة من تواقيع التفتيش المتعمق على الرزمة. وتدعى أيضاً مكتبة بروتوكول التفتيش المتعمق على الرزمة لأن التواقيع يمكن أن تُستخدم عادة لتحديد هوية بروتوكول.

16.2.3 واصف التدفق (المعروف أيضاً بشروط مستوى التدفق): مجموعة من شروط القاعدة التي تُستخدم لتحديد هوية نوع معين من التدفق (وفقاً للفقرة 3.1.3) من الحركة الخاضعة للتفتيش.

الملاحظـــة 1 – يوسع هذا التعريف لواصف التدفق التعريف الوارد في التوصية [b-ITU-T Y.2121] بعناصر إضافية على النحو الموضح في الفقرة 3.

الملاحظـــة 2 – للاطلاع على مزيد من المناقشة المعيارية لواصف التدفق على النحو المستخدم في هذه التوصية، انظر الملحق A.

17.2.3 محدد هوية التدفق وفق بروتوكول IPFIX: مجموعة من قيم مفاتيح تدفق IPFIX المستخدمة جنباً إلى جنب مع واصف التدفق للتعرف على تدفق معين.

18.2.3 مفتاح التدفق وفق بروتوكول IPFIX: كل واحد من عناصر المعلومات من واصف التدفق المستخدمة في عمليات تحديد هوية التدفق القائمة على IPFIX (وفقاً لمعيار [IETF RFC 5101]).

ملاحظـــة – يتسق تعريف مفتاح التدفق وفق بروتوكول IPFIX من حيث الدلالات اللغوية مع تعريف مفتاح التدفق المحدد في بروتوكول IPFIX [IETF RFC 5101]. والفرق الوحيد بين المصطلحين هو أن نطاق التعريف الوارد في هذه الوثيقة ينحصر في واصف التدفق.

19.2.3 التفتيش على رأسية الطبقة ($L_{3,4}$HI): معالجة قاعدة (أو قواعد) السياسة المتبعة بشروط هذه السياسة التي لا تتضمن إلا عناصر معلومات التحكم في البروتوكول (PCI) في طبقة الشبكة و/أو طبقة النقل.

20.2.3 الطبقة L4+ التفتيش على الرأسية (L_4+HI): معالجة قاعدة (أو قواعد) السياسة المتبعة بشروط هذه السياسة التي لا تتضمن إلا عناصر معلومات التحكم في البروتوكول (PCI) فوق طبقة النقل.

21.2.3 التفتيش على حمولة الطبقة L4 (L_4PI): معالجة قاعدة (أو قواعد) السياسة المتبعة بشروط هذه السياسة التي لا تتضمن إلا حمولة النقل والتي قد تكون "بيانات التطبيق" لبروتوكولات تطبيق معين (على سبيل المثال، بروتوكول استهلال الدورة (SIP)).

ملاحظة – يجمع التفتيش على حمولة الطبقة L_4 (L_4PI) بين شروط السياسة المتبعة في L_4+HI وL_7PI.

22.2.3 التفتيش على حمولة الطبقة L7 (L_7PI): معالجة قاعدة (أو قواعد) السياسة المتبعة استناداً إلى بيانات التطبيق.

23.2.3 الحمولة: وحدة البيانات التالية لعناصر الرأسية في رزمة، والمستبعِدة للعناصر الاختيارية في نهاية الرزمة (على سبيل المثال، عناصر الملء وبيانات الذيل والمجموع التدقيقي).

الملاحظة 1 – وهكذا، فإن مفهوم الحمولة هو مرادف لوحدة بيانات الخدمة (SDU) في النموذج المرجعي الأساسي للتوصيل البيني للأنظمة المفتوحة (OSI-BRM) [ITU-T X.200]، والرزمة هي مرادف لوحدة بيانات البروتوكول (PDU)، وتشمل معلومات التحكم في البروتوكول (PCI) جميع عناصر رأسية الرزمة وبيانات الذيل. وخلاصة القول، "PDU = PCI + SDU".

الملاحظة 2 – يتسم مفهوم الحمولة بخصوصية طبقة بروتوكول معينة (على سبيل المثال، يشير الرمز، Lx–الحمولة، إلى الحمولة في طبقة × من البروتوكول). وكذلك الأمر بالنسبة إلى Lx-SDU وLx-PDU وLx-PCI.

4 المختصرات

تستخدم هذه التوصية المختصرات التالية:

AH رأسية الاستيقان (*Authentication Header*)

BRM نموذج مرجعي أساسي (*Basic Reference Model*)

DCCP بروتوكول التحكم في ازدحام وحدات البيانات (*Datagram Congestion Control Protocol*)

DPI التفتيش المتعمق على الرزمة (*Deep Packet Inspection*)

DPI-FE الكيان الوظيفي للتفتيش المتعمق على الرزمة (*DPI Functional Entity*)

DPI-PDFE الكيان الوظيفي المعني بقرار سياسة التفتيش المتعمق على الرزمة (*DPI Policy Decision Functional Entity*)

DPI-PE الكيان المادي للتفتيش المتعمق على الرزمة (*DPI Physical Entity*)

DPI-PIB قاعدة معلومات سياسة التفتيش المتعمق على الرزمة (*DPI Policy Information Base*)

ESP الحمولة الأمنية المغلِّفة (*Encapsulating Security Payload*)

ET الاتصالات في حالات الطوارئ (*Emergency Telecommunications*)

FPA تحليل منطقة الحمولة كاملة (*Full Payload area Analysis*)

FSL لغة توصيف المرشاح (*Filter Specification Language*)

HTTP بروتوكول نقل النص التشعبي (*Hypertext Transfer Protocol*)

IANA هيئة تخصيص أرقام الإنترنت (*Internet Assigned Numbers Authority*)

IE عناصر معلومات (*Information Elements*)

IP بروتوكول الإنترنت (*Internet Protocol*)

IPFIX تصدير معلومات تدفق بروتوكول الإنترنت (*IP Flow Information Export*)

IS في الخدمة (*In-Service*)

L-PDF وظيفة قرار السياسة المتبعة محلياً (*Local PDF*)

MPLS تبديل الوسم بعدة بروتوكولات (*Multi Protocol Label Switching*)

NGN شبكة الجيل التالي (*Next Generation Network*)

NMS نظام إدارة الشبكة (*Network Management System*)

OGP بروتوكول مفتوح للألعاب (*Open Game Protocol*)

OoS خارج الخدمة (*Out-of-Service*)

OSI-BRM التوصيل البيني للأنظمة المفتوحة – نموذج مرجعي أساسي (*Open Systems Interconnection – Basic Reference Model*)

P2P بين النظراء (*Peer to Peer*)

PCC التحكم في السياسة المتبعة والترسيم (*Policy and Charging Control*)

PCI معلومات التحكم في بروتوكول (*Protocol Control Information*)

PDF وظيفة قرار السياسة المتبعة (*Policy Decision Function*)

PDU وحدة بيانات البروتوكول (*Protocol Data Unit*)

PEL لغة التعبير عن السياسة المتبعة (*Policy Expression Language*)

PFF وظيفة إعادة تسيير الرزمة (*Packet Forwarding Function*)

PIB قاعدة معلومات السياسة المتبعة (*Policy Information Base*)

PPA تحليل منطقة الحمولة (*Payload area Analysis*)

PSAMP أخذ عينات من الرزم (*Packet Sampling*)

PSL لغة توصيف السياسة المتبعة (*Policy Specification Language*)

RACF وظائف التحكم في الموارد والقبول (*Resource and Admission Control Functions*)

RACS النظام الفرعي للتحكم في الموارد والقبول (*Resource and Admission Control Subsystem*)

R-PDF الوظيفة البعيدة لقرار السياسة المتبعة (أي وظيفة إعادة تسيير الرزمة الواقعة بعيداً من منظور عقدة التفتيش المتعمق على الرزمة) (*Remote PDF (i.e., PDF remotely located from DPI node perspective)*)

RTP بروتوكول النقل في الوقت الفعلي (*Real-time Transport Protocol*)

SA ترابط أمني (IPsec) (*Security Association (IPsec)*)

SCTP بروتوكول إرسال التحكم في قطار البتات (*Stream Control Transmission Protocol*)

SDU وحدة بيانات الخدمة (*Service Data Unit*)

SigComp ضغط التشوير (*Signaling Compression*)

SIP بروتوكول استهلال الدورة (*Session Initiation Protocol*)

SPI مؤشر معلمة الأمن (IPsec) (*Security Parameter Index (IPsec)*)

TCP بروتوكول التحكم في الإرسال (*Transmission Control Protocol*)

TISPAN خدمات وبروتوكولات الاتصالات والإنترنت للربط الشبكي المتقدم
(*Telecommunication and Internet Converged Services and Protocols for Advanced Networking*)

UDP بروتوكول وحدة بيانات المستخدم (*User Datagram Protocol*)

5 اصطلاحات

تتضمن هذه الوثيقة قائمة من البنود الموسومة بشكل *R-x/y* حيث يشير *x* إلى رقم الفقرة و*y* إلى رقم ضمن تلك الفقرة. وتستخدم هذه البنود الكلمات الأساسية التالية التي تؤدي المعاني المبينة أدناه:

"يجب" أو "يلزم" أو "مطلوب" كلمات تدل على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم المطابقة مع هذه الوثيقة.

"يجب ألا" أو "يلزم ألا" أو "يحظر" كلمات تدل على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم المطابقة مع هذه الوثيقة.

وكلمة "يُوصَى" تدل على متطلب يوصى به لكنه غير إلزامي بالمطلق. وبالتالي لا حاجة تدعو لتوفر هذا المتطلب لزعم المطابقة.

وكلمات "يمكن اختيارياً" أو "يجوز" أو "من الجائز" أو "ربما" تدل على مطلب خياري مسموح به دون أن ينطوي على أي توصية به. ولا ترمي هذه المصطلحات إلى إلزام التطبيق بتوفير هذا الخيار الذي يمكن أن يوفره مشغل الشبكة/مقدم الخدمة خيارياً. بل إن المصنّع يمكنه إدراج هذا الخيار وزعم مطابقة المواصفة في نفس الوقت.

وفي متن هذه التوصية وملحقاتها، تظهر في بعض الأحيان كلمات يتعين، ويتعين ألا، وينبغي، ويمكن. وفي هذه الحالة يكون تأويلها، على التوالي، على "يجب" أو "يلزم" أو "مطلوب"، و"يجب ألا" أو "يلزم ألا" أو "يحظر"، و"يوصي" و"ربما" أو "يجوز" أو "من الجائز". ويأوّل انتفاء القصد المعياري عند ظهور مثل هذه العبارات أو الكلمات الرئيسية في تذييل أو في مادة موسومة صراحةً على أنها إعلامية.

6 متطلبات الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE)

1.6 تحديد هوية التدفق والتطبيق

R-6.1/1: يجب على الكيان الوظيفي للتفتيش المتعمق على الرزمة أن يحدد هوية التطبيق.

R-6.1/2: يجب على الكيان الوظيفي للتفتيش المتعمق على الرزمة أن يدعم أنواع مختلفة من قواعد سياسة التفتيش المتعمق على الرزمة.

R-6.1/3: يجب على الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يحدد هوية التطبيق بالكشف على حمولة التطبيق.

R-6.1/4: مطلوب من شروط مستوى تطبيق التفتيش المتعمق على الرزمة (وشروط مستوى التدفق الاختيارية) أن تسمح بتحديد هوية التطبيق على أساس اتجاه الحركة الأحادي (التفتيش المتعمق على الرزمة أحادي الاتجاه) لجميع التطبيقات أحادية الاتجاه وللتطبيقات ثنائية الاتجاه بشرط أن تسمح الحركة أحادية الاتجاه بتحديد الهوية على نحو لا لبس فيه.

R-6.1/5: يمكن اختيارياً لشروط مستوى تطبيق التفتيش المتعمق على الرزمة (وشروط مستوى التدفق الاختيارية) أن تسمح بتحديد هوية التطبيق على أساس ثنائية اتجاه الحركة (التفتيش المتعمق على الرزمة ثنائي الاتجاه).

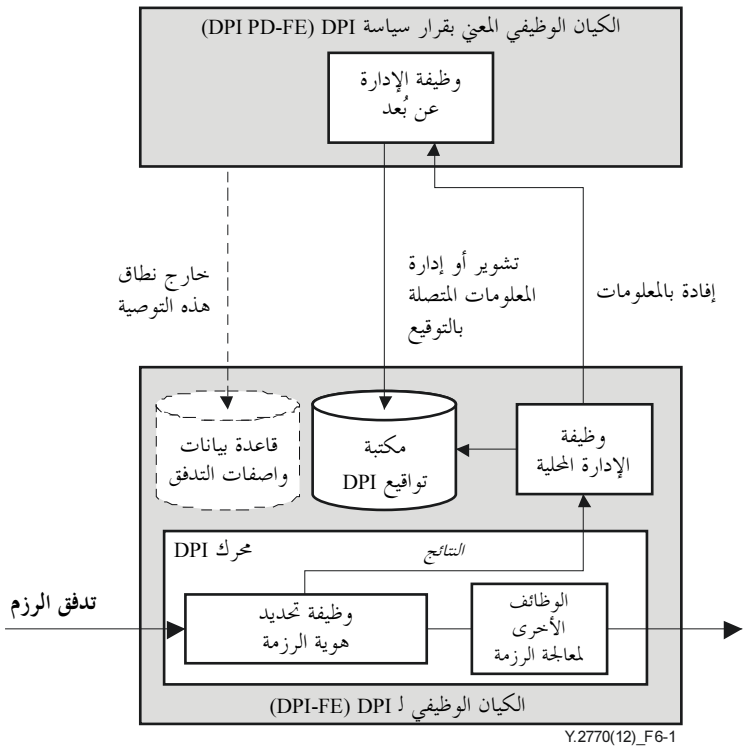
R-6.1/6: يوصى بعنصر (أو عناصر) المعلومات المستخدمة في شروط مستوى التدفق للالتزام بمعيار [b-IETF RFC 5102]، على النحو المسجَّل لدى هيئة تخصيص أرقام الإنترنت [b-IETF IANA IPFIX]. وفي مثل هذه الحالة، يوصى بأن تتضمن عناصر المعلومات عناصر معلومات IPFIX المتعلقة بطبقات بروتوكول الوصلة (L2) والشبكة (L3) والنقل (L4)، باتباع المعمارية الأساسية لبروتوكول IETF ذي الطبقات.

ملاحظـــة – يمكن اختيارياً توسيع سجل عناصر معلومات IPFIX لدى هيئة تخصيص أرقام الإنترنت (IANA) (من جانب فريق مهام هندسة الإنترنت (IETF)) ليشمل عناصر إضافية. فسجل IANA الحالي (حتى نهاية عام 2011) تنقصه عناصر معلومات عن بروتوكولات الطبقة L4 عدا بروتوكولي UDP وTCP (ومن أمثلة النقص، عناصر معلومات عن بروتوكولي SCTP وDCCP).

R-6.1/7: يمكن اختيارياً لعنصر (أو عناصر) المعلومات أن تكون عناصر معلومات غير تلك ذات الصلة بالطبقة L2 أو L3 أو L4 خارج سجل IPFIX (وتسمى عناصر معلومات خاصة بمؤسسة في بروتوكول IPFIX [IETF RFC 5101]).

2.6 إدارة توقيع التفتيش المتعمق على الرزمة (DPI)

تعرّف هذه الفقرة المتطلبات المتعلقة بالعمليات على مكتبة تواقيع التفتيش المتعمق على الرزمة (DPI). ويمكن للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أو لكيان شبكي بعيد أن يبادر بمثل هذه العمليات محلياً (انظر الشكل 6-1). ويمكن لجميع الأنماط الممكنة من الكيانات الشبكية البعيدة أن تُعتبر من الناحية التجريدية بمثابة الكيان الوظيفي المعني بقرار سياسة التفتيش المتعمق على الرزمة الذي يقرر القواعد القائمة على التوقيع الواجب إنفاذها في الكيان DPI-FE.



الشكل 6-1 – إدارة توقيع التفتيش المتعمق على الرزمة (DPI) في نطاق مثال معمارية الكيان الوظيفي للتفتيش المتعمق على الرزمة (انظر أيضاً الشكل 8-2 فيما يتعلق بالسطوح البينية الداخلية)

يرتبط الكيان الوظيفي المعني بقرار سياسة التفتيش المتعمق على الرزمة مع وظائف التحكم في الموارد والقبول (RACF) (في حالة وجود شبكة الجيل التالي مع وظائف التحكم في الموارد والقبول)، ولكن مواصفته تقع خارج نطاق هذه التوصية. ويرد في الشكل 6-1 لأنه يحتوي على وظائف الإدارة عن بُعد في الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE).

1.2.6 متطلبات التوقيع العامة

R-6.2.1/1: يجب أن تخزَّن تواقيع التفتيش المتعمق على الرزمة (DPI) في *مكتبة تواقيع DPI* التي تشكل كياناً فرعياً في الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE).

ملاحظـــة – يرتكز الأساس المنطقي لمكتبة تواقيع التفتيش المتعمق على الرزمة إلى أن وظيفة تحديد هوية الرزمة تتطلب إمكانية الوصول الفوري إلى محتوى قاعدة البيانات.

ويمكن استخدام توقيع التفتيش المتعمق على الرزمة (DPI) من أجل ما يلي:

- تحديد تقريبي للهوية (السلوكية أو الاستدلالية مثلاً، وغيرها)؛
- وتحديد دقيق تحديد للهوية (مثل قواعد المطابقة التامة).

وتقع اللغة (الرسمية أو السلوكية) المستخدمة لتحديد قواعد سياسة التفتيش المتعمق على الرزمة (DPI)، فضلاً عن قواعد المطابقة نفسها، خارج مجال تطبيق هذه التوصية. ولا تحدد هذه التوصية إلا وجود مكتبة تواقيع التفتيش المتعمق على الرزمة، وماهية التواقيع الموجودة، ووظائف إدارة المكتبة.

R-6.2.1/2: ويجب الحفاظ على مكتبة تواقيع التفتيش المتعمق على الرزمة بشكل آمن وغير مرئي للمستخدمين غير المخولين.

2.2.6 إدارة مكتبة تواقيع التفتيش المتعمق على الرزمة (DPI)

تحدد هذه الفقرة متطلبات مكتبة تواقيع التفتيش المتعمق على الرزمة.

1.2.2.6 إضافة تواقيع جديدة

R-6.2.2.1/1: تلزم القدرة على إضافة تواقيع DPI جديدة إلى مكتبة تواقيع التفتيش المتعمق على الرزمة.

2.2.2.6 العمليات على التواقيع الموجودة

R-6.2.2.2/1: تلزم القدرة على تعديل (تحديث) التواقيع الموجودة في مكتبة تواقيع التفتيش المتعمق على الرزمة.

R-6.2.2.2/2: تلزم القدرة على تمكين وتعطيل تواقيع DPI معينة في مكتبة تواقيع التفتيش المتعمق على الرزمة.

R-6.2.2.2/3: تلزم القدرة على حذف (إزالة) تواقيع DPI معينة في مكتبة تواقيع التفتيش المتعمق على الرزمة.

3.2.2.6 تبادل نسق القاعدة عبر سطح بيني خارجي

R-6.2.2.3/1: يمكن اختيارياً اتباع أي نسق قاعدة (انظر أيضاً الفقرة 2.1) لتوقيع التفتيش المتعمق على الرزمة من أجل تحديد هوية تطبيق عبر سطوح بينية خارجية (أي *e1* و*e2* في الشكل 8-1).

3.2.6 موقع وظيفة الإدارة

R-6.2.3/1: يجب تنفيذ إجراءات إدارة توقيع التفتيش المتعمق على الرزمة المحددة في الفقرة 2.2.6 محلياً من موقع الكيان الوظيفي للتفتيش المتعمق على الرزمة أو من موقع بعيد أو من كلا الموقعين (انظر الشكل 6-1).

4.2.6 الشروع في إجراءات الإدارة

R-6.2.4/1: يلزم دعم أسلوب الدفع بشأن عمليات توقيع التفتيش المتعمق على الرزمة (DPI) عند البدء بهذه العمليات عن بُعد (على سبيل المثال، من جانب الكيان الوظيفي المعني بقرار سياسة التفتيش المتعمق على الرزمة (DPI-PDFE) في الشكل 6-1).

R-6.2.4/2: يلزم دعم أسلوب الجذب بشأن عمليات توقيع التفتيش المتعمق على الرزمة (DPI) عند البدء بهذه العمليات محلياً. ومؤدى مفهوم الجذب أن وظيفة الإدارة المحلية للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) تطلب إلى الكيان الوظيفي المعني بقرار سياسة التفتيش المتعمق على الرزمة (DPI-PDFE) تنفيذ إجراء إداري على توقيع جديد أو قائم.

أما كيف يُفعَّل الكيان الوظيفي للتفتيش المتعمق على الرزمة طلباً فهو خارج نطاق هذه التوصية.

3.6 جوانب التفتيش على الحركة

تتناول هذه الفقرة الجوانب المتعلقة بأنماط الحركة الخاضعة للتفتيش المتعمق على الرزمة (DPI).

1.3.6 جوانب تحديد هوية التدفق

R-6.3.1/1: يوصى أن يدعم الكيان الوظيفي للتفتيش المتعمق على الرزمة تحديد هوية التطبيقات، من دون التفتيش على مستوى التدفق.

R-6.3.1/2: يمكن اختيارياً لأي سيناريو تفتيش متعمق على الرزمة (DPI) أن يكون في البداية مستقلاً عن التدفق، أي أن تخلو قاعدة سياسة التفتيش المتعمق على الرزمة المقدمة إلى الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) من واصف تدفق. بيد أن القاعدة تستطيع أن تطلب جمع معلومات التدفق التي تسترعي الاهتمام.

R-6.3.1/3: يلزم مثل هذا الطلب لتوفير مفتاح تدفق IPFIX بالإضافة إلى الإتمام الاختياري لنقص معلومات التدفق.

R-6.3.1/4: يمكن اختيارياً للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يتطلب الاعتراف الكامل بمحدد هوية تدفق IPFIX على أساس مفتاح تدفق IPFIX معين والتفتيش على رزم متعددة لاحقة.

R-6.3.1/5: يمكن اختيارياً لإجراء الإبلاغ من جانب الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) إلى كيان شبكي بعيد أن يكون مشروطاً (كأن يكون مفعَّلاً بحدث معين، أو متحكَّماً فيه بمؤقت، وما إلى ذلك).

2.3.6 جوانب التفتيش المتعمق على الرزمة (DPI) العليمة بكدسة البروتوكول وغير العليمة بكدسة البروتوكول

تتولى وظيفة الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) مسؤولية تحديد هوية تطبيق وتعنى بعمليات المقارنة والبحث استناداً إلى توقيع التفتيش المتعمق على الرزمة (DPI) وبالقياس مع رزمة واردة (بوحدة بيانات بروتوكول (PDU)). وهناك خياران: إما أن يكون الكيان الوظيفي للتفتيش المتعمق على الرزمة عليماً بهيكل PDU الداخلي (أي "كيان DPI-FE العليم بكدسة البروتوكول") أو غير عليم بالهيكل ("*كيان DPI-FE غير العليم بكدسة البروتوكول*").

وقد يقدم الخياران كلاهما النتيجة نفسها من حيث تحديد الهوية، ويتعادلان وظيفياً. ويكمن الفرق الرئيسي في أن منطق تحديد الهوية العليم بكدسة البروتوكول قد يكون أكثر كفاءة.

من المفيد التمييز بين النوعين التاليين من التحليل بشأن الكفاءة التشغيلية (أي تحديد هوية التطبيق وتحديد هوية التدفق اختيارياً):

أ) تحليل منطقة الحمولة المحددة مسبقاً (PPA): عند تطابق (تدفق) رزم مع تطبيق معروف ذي هيكل حمولة محدد بوضوح، يمكن للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يفتش على الموقع الثابت المحدد سلفاً للحمولة (أي أسلوب التفتيش على الرزمة العليم بكدسة البروتوكول).

ب) تحليل كامل منطقة الحمولة (FPA): عند عدم تطابق (تدفق) رزم مع تطبيق معروف أو كون هيكل الحمولة غير محدد بوضوح، يقوم الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) بالتفتيش على "كامل منطقة الحمولة" (أي أسلوب التفتيش على الرزمة غير العليم بكدسة البروتوكول).

ويمكن تطبيق تحليلي PPA وFPA كليهما على تدفق الحركة نفسه.

R-6.3.2/1: يوصى بأن يدعم الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) تحديد هوية التطبيق العليم بكدسة البروتوكول.

R-6.3.2/2: يوصى بأن يدعم الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) تحديد هوية التطبيق غير العليم بكدسة البروتوكول.

R-6.3.2/3: يجب على الكيان الوظيفي للتفتيش المتعمق على الرزمة أن يحدد هوية التطبيقات التي تعمل فوق كدستي بروتوكولي الإصدارين الرابع والسادس من بروتوكول الإنترنت (IPv4 وIPv6)، ويمكنه القيام بذلك اختيارياً بالنسبة للتطبيقات التي تعمل كدسات البروتوكولات الأساسية الأخرى.

R-6.3.2/4: يوصى بأن يدعم الكيان الوظيفي للتفتيش المتعمق على الرزمة التطبيقات في الحركة المستبطَنة؛ مثل الحركة المغلفة أو الممررة في نفق.

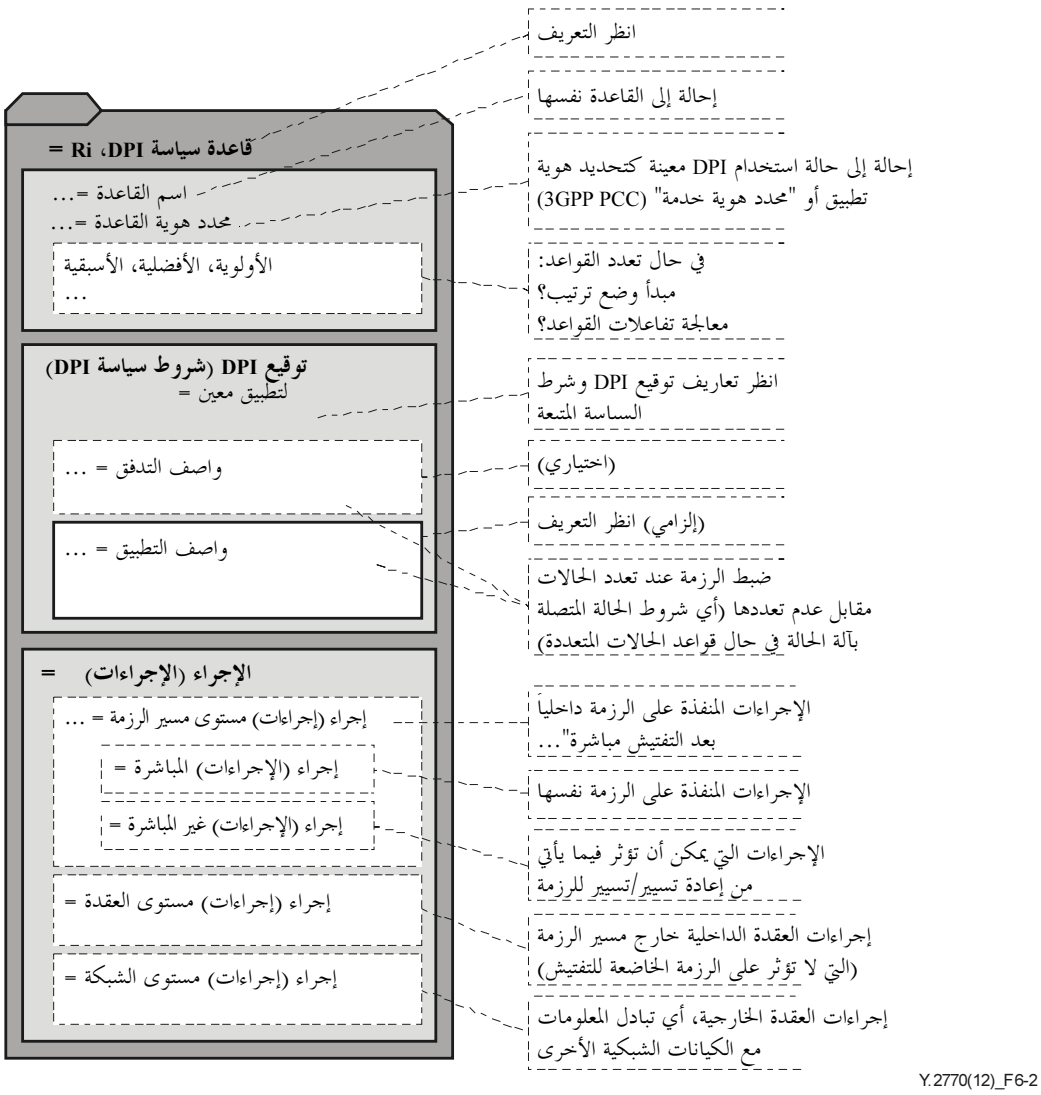
3.3.6 جوانب إجراءات قاعدة سياسة التفتيش المتعمق على الرزمة (DPI)

1.3.3.6 معلومات أساسية

يمكن تنفيذ إجراءات سياسة التفتيش المتعمق على الرزمة (DPI) على مستويات تراتبية مختلفة، مثل الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) ووظائف قرار السياسة المتبعة محلياً وعن بُعد، ويمكن أن تشمل ما يلي على سبيل المثال:

1) الإجراءات على مستوى مسير الرزمة (من جانب الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE)):
   أ) قبول الرزمة وإعادة تسييرها إلى وظيفة إعادة تسيير الرزمة (PFF) (إجراء شرطي في أسلوب التفتيش المتعمق على الرزمة (DPI) ضمن المسير فقط)؛
   ب) نبذ الرزمة (بصمت أو بغير ذلك)؛
   ج) إعادة توجيه الرزمة إلى السطوح البينية الأخرى للخرج؛
   د) استنساخ/تكرار الرزمة في السطوح البينية الأخرى للخرج؛
   هـ) تصنيف الحركة، والقياسات المحلية، والإبلاغ عن بيانات القياس؛
   و) طرائق تحديد الأولويات، والحجب، والقولبة، والجدولة الزمنية في فرادى الرزم.
2) الإجراءات على مستوى العقدة (باشتراك وظيفة قرار السياسة المتبعة محلياً (L-PDF)):
   أ) البناء الدينامي للقواعد الجديدة لسياسة التفتيش المتعمق على الرزمة (DPI) و/أو تعديل القواعد القائمة (المخزنة في قاعدة معلومات سياسة التفتيش المتعمق على الرزمة (DPI-PIB))؛
   ب) القيام بتسجيل/تتبع البيانات وإبلاغ إدارة السياسة المتبعة (انظر الفقرة 2.11.2 في المعيار [b-IETF RFC 3871])؛
   ج) الكشف والإبلاغ عن التطبيقات التي يتعذر تحديد هويتها؛
   د) تبليغ أنظمة كشف الاقتحام (على سبيل المثال، عن طريق الإبلاغ عن عينات الحركة، والرزم المشبوهة).
3) إجراءات على مستوى الشبكة (عبر الوظيفة البعيدة لقرار السياسة المتبعة (R-PDF)):
   أ) إدارة الموارد والتحكم في القبول واصطفاء المستوى العالي (على مستوى الأنظمة الفرعية للشبكة (مثل تلك المحددة من أجل معايير RACF في التوصية [ITU-T Y.2111] وETSI TISPAN RACS [b-ETSI ES 282 003] و3GPP PCC [b-ETSI TS 123 203])؛
   ب) استيفاء رسوم عن المحتوى حسب أنواع تطبيقات المشتركين (على سبيل المثال، بروتوكول RADIUS أو بروتوكول القطر IETF (Diameter)).

ويرد في الشكل 6-2 مزيد من الشرح لمبدأ الهيكلة المذكورة أعلاه من خلال نسق سياسة عامة تفصيلية (مقابل تلك التي جرى التعريف بها في الفقرة 2.1):



الشكل 6-2 – مثال على نسق سياسة عامة تفصيلية (بالمقارنة مع الشكل 1-2)

ويقع التقابل بين الإجراءات المحددة وبين الشروط خارج نطاق هذه التوصية.

2.3.3.6 المتطلبات

R-6.3.3.2/1: ما أن يحدد الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) هوية تطبيق، يمكن اختيارياً استخراج المعلومات عن تطبيق معين.

على سبيل المثال، الرابط الموحد للمورد (URL) في بروتوكول نقل النص التشعبي (HTTP)، أو نسق وسائط ("نمط كودك") في بروتوكول النقل في الوقت الفعلي (RTP)، أو محدد هوية دورة RTP (على سبيل المثال، مصدر التزامن (SSRC) للنقطة الطرفية في مصدر RTP).

R-6.3.3.2/2: يمكن اختيارياً للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يعمل إلى جانب وظيفة قياس التدفق، ومثال ذلك، عملية القياس وفق بروتوكول IPFIX [IETF RFC 5101] وبعض قدرات الاصطفاء مثل المعيار [b-IETF RFC 5476].

ملاحظـــة – عادةً ما تملأ عملية القياس هذه عناصر معلومات IPFIX التالية (المستخدَمة كمفاتيح تدفق): sourceIPv6Address وdestinationIPv6Address وsourceIPv4Address وdestinationIPv4Address وprotocolIdentifier وsourceTransportPort، وdestinationTransportPort، وما إلى ذلك. غير أن دور الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) يتمثل في وسم التطبيق واستكمال محدد هوية التدفق (على أساس مفتاح تدفق IPFIX معين، انظر أيضاً الشكل A.1).

4.6 قدرة الإبلاغ

يتعلق الإبلاغ بإخطار (على سبيل المثال، نتيجة لحدث معين كشفه الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE)) كيان وظيفي آخر يقع عادة في عنصر شبكي بعيد (في مستوي المستخدم أو التحكم أو الإدارة). ويمكن للكيان الوظيفي للتفتيش المتعمق على الرزمة أن يوفر سطوح بينية متعددة للإبلاغ دعماً "لأنماط مختلفة من الأحداث".

1.4.6 إبلاغ نظام إدارة الشبكة (NMS)

1.1.4.6 السطح البيني والبروتوكول للإبلاغ

R-6.4.1.1/1: يوصى بأن يتّبع بروتوكول التصدير مواصفة IPFIX [IETF RFC 5101]، ويمكن اختيارياً أن يتّبع توسعات IPFIX.

R-6.4.1.1/2: يمكن اختيارياً أن يتّبع بروتوكول التصدير مواصفة IPFIX [b-IETF RFC 5103]، في حالة وجود تدفقات ثنائية الاتجاه.

R-6.4.1.1/3: يوصى بأن تستخدم بروتوكولات التصدير القائمة على IPFIX السطح البيني الخارجي e2 (انظر الشكل 8-1).

2.1.4.6 المعلومات المبلَّغة

R-6.4.1.2/1: يجب على الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يبلغ مستوي إدارة التفتيش المتعمق على الرزمة بنتائج التفتيش (مثل وسم التطبيق وعناصر معلومات خاصة بالتطبيق) مع المعلومات الخاصة بالتدفق. ويمكن اختيارياً تصدير قيم مفتاح التدفق المحدَّثة محلياً (بما في ذلك الحقول النمطية من وظيفة تدفق القياس) إلى وظيفة قرار السياسة المتبعة (على سبيل المثال الكيان الوظيفي المعني بقرار سياسة المتبعة (PD-FE) المحدد في التوصية [ITU-T Y.2111]).

R-6.4.1.2/2: يوصى بأن تعيد المعلومات المبلَّغة استخدام عناصر معلومات IPFIX ([b-IETF IANA IPFIX])، التي جرى توصيفها في البداية في نموذج معلومات IPFIX [b-IETF RFC 5102].

وتوصَّف المعلومات الخاصة بالتدفق في نموذج معلومات IPFIX [b-IETF RFC 5102]، على سبيل المثال:

1) المعلومات الخاصة بتطبيق:
   - وسم التطبيق؛
   - والحقول المستخرجة مثل نسق وسائط في بروتوكول النقل في الوقت الفعلي (RTP) ومصدر التزامن في بروتوكول النقل في الوقت الفعلي (RTP SSRC).
2) حقول رأسية L3/L4 المقابلة لعناوين بروتوكول الإنترنت، ومنافذ الطبقة L4 (على سبيل المثال، TCP أو UDP، الملاحظة 1)، ونوع البروتوكول؛
3) معلومات عن الأداء (مثل المقاييس والإحصاءات) وتعداد البايتات وتعداد الرزم والحد الأقصى لمقاس الحزمة (الملاحظة 2)؛
4) معلومات عن الوقت: وقت بدء التدفق، وقت نهاية التدفق؛
5) المعلومات المرتبطة بالرزمة: القفزة التالية ومقاس الرزمة (الملاحظة 3)؛

الملاحظة 1 – بعض عناصر المعلومات المذكورة ليست مدرجة (بعد) في سجل IPFIX لدى هيئة تخصيص أرقام الإنترنت (IANA)، ولكنها صحيحة في سياق هذه التوصية.

الملاحظة 2 – يمكن توليد المعلومات الخاصة بالتدفق بواسطة آلية أخذ العينات من الرزمة (PSAMP)، ولكن عندما تصدَّر مثل هذه النتائج إلى نظام إدارة الشبكة (NMS)، يوصى بإضافة المعلومات الخاصة بالتطبيق.

الملاحظة 3 – قد تدعو الضرورة تسجيل عناصر معلومات جديدة في سجل IPFIX لدى هيئة تخصيص أرقام الإنترنت (IANA)، وفقاً للقسم 7 المعنون "اعتبارات هيئة تخصيص أرقام الإنترنت" في المعيار [b-IETF RFC 5102].

2.4.6 الإبلاغ عن تطبيق جديد أو مجهول أو غير صحيح

1.2.4.6 خصائص هذه الحركة

هناك فروق دقيقة بين أنماط هذه التطبيقات. ويمكن تشخيصها بتقصي خصائص معينة، مما يؤدي إلى شروط مختلفة في مستوى التطبيق لكشف هذه الخصائص:

- تطبيق جديد: كإصدار جديد لتطبيق أو إصدار جديد لعنصر معلومات خاص بتطبيق (مثل إصدار جديد للعبة ضمن البروتوكول المفتوح للألعاب (OGP)) أو إصدار جديد لبروتوكول، علماً بأن مفهوم "الجديد" يعكس منظور خدمة التفتيش المتعمق على الرزمة (DPI) (الذي قد يكون مبنياً على تاريخ من خدمات سابقة في التفتيش المتعمق على الرزمة)؛
- تطبيق مجهول: مثل نمط مجهول من الرزم أو بروتوكول مجهول أو "تطبيق" مجهول؛
- تطبيق غير صحيح: مثل رزمة حاملة لقواعد لغة بروتوكول غير صحيحة (ملاحظة)، إلخ.

ملاحظـــة – يمكن استغلال قواعد تركيب لغة البروتوكول غير الصحيحة لشن هجوم يخل بأمن البروتوكول. وعادة ما تكون البروتوكولات المتضررة تلك المنتهية في معدات المستخدم (مثل بروتوكولات التشوير).

2.2.4.6 متطلبات الإبلاغ

R-6.4.2.2/1: يمكن اختيارياً للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يدعم الإبلاغ عن تطبيق جديد أو مجهول أو غير صحيح بعد التفتيش على الحركة.

3.4.6 الإبلاغ عن حركة شاذة

R-6.4.3/1: يمكن اختيارياً للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يوفر قدرة الإبلاغ المتصلة بكشف الحركة الشاذة عند كشفها.

وتعرَّف الحركة الشاذة على أنها الحركة التي لا ترتبط مع أصناف الحركة الطبيعية. وصنف الحركة الطبيعية هو مجموعة الحركة التي تطابق الخصائص الإحصائية القائمة لتطبيقات واضحة المعالم مثل الوقت الفاصل بين ورود رزمة وأخرى، أو ترتيب الورود، أو مقاس وحدة بيانات البروتوكول (PDU) لطبقة بروتوكول معينة، أو حجم الحمولة، أو حجم الحركة (في طبقة بروتوكول معينة).

4.4.6 الإبلاغ عن الأحداث المتصلة بالكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE)

تصف هذه الفقرة الأحداث المتعلقة بالحالة التشغيلية لكيان التفتيش المتعمق على الرزمة (DPI) ومتطلبات الإبلاغ ذات الصلة.

1.4.4.6 أحداث التعطل المتصلة بالسلوك غير الصحيح للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE)

تتمثل أبسط طريقة لإيضاح حالة إدارة الكيان الوظيفي للتفتيش المتعمق على الرزمة في عرضها بدلالة حالتين "في الخدمة" (IS) و"خارج الخدمة" (OoS).

R-6.4.4.1/1: يوصى بإدارة التفتيش المتعمق على الرزمة (DPI) على أساس أرقى المعايير (ومثالها [ITU-T X.731] و[b-IETF RFC 4268]) ويوصى بأن تدعم هذه الإدارة حالتي الإدارة "في الخدمة" (IS) و"خارج الخدمة" (OoS) على أقل تقدير.

R-6.4.4.1/2: يمكن اختيارياً لأي تعطل في الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE)، إن لم تكن معماريته مزودة برديف، أن يتسبب بالانتقال من حالة "في الخدمة" (IS) إلى حالة "خارج الخدمة" (OoS). ويوصى بالإبلاغ عن هذه الأحداث.

2.4.4.6 الأحداث المتعلقة بإدارة تعطل الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE)

يوفر الكيان الوظيفي للتفتيش المتعمق على الرزمة سطوح بينية شبكية لحركة الدخول والخروج، وقد يحدث تعطل في هذه السطوح البينية.

R-6.4.4.2/1: يوصى بأن يدعم الكيان الوظيفي للتفتيش المتعمق على الرزمة وظيفة الإبلاغ عن إنذار على النحو المحدد في التوصية [b-ITU-T X.734].

3.4.4.6 الأحداث المتصلة بتسجيل الكيان الوظيفي للتفتيش المتعمق على الرزمة

R-6.4.4.3/1: يمكن اختيارياً للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يدعم قدرة نظام تسجيل مثل Syslog [b-IETF RFC 5424]. وفي مثل هذه الحالة، يكون الكيان الوظيفي للتفتيش المتعمق على الرزمة هو نقطة منشأ رسائل Syslog.

وتجدر الإشارة إلى أنه في الحالة التي يحمل فيها تدفق الرزمة المفتشَة حركة التسجيل، لا يكون الكيان الوظيفي للتفتيش المتعمق على الرزمة لا نقطة منشأ الرسائل ولا نقطة منتهاها. وبعبارة أخرى، يمكن أن يستند مفتاح البحث عن تدفق الرزمة هذا إلى واصف تطبيق (على صلة بطبقة تطبيق syslog) وإلى واصف تدفق IPFIX (على صلة بأسلوب نقل syslog المختار). ويمكن الاطلاع على مزيد من المعلومات في المعيارين [b-IETF RFC 5424] و[b-IETF RFC 5426].

4.4.4.6 الأحداث المتصلة بحالة الحمل واستهلاك الموارد في الكيان المادي للتفتيش المتعمق على الرزمة

يملك الكيان المادي للتفتيش المتعمق على الرزمة (DPI-PE) موارد محدودة لمعالجة التفتيش المتعمق على الرزمة. وتعتمد حيثيات المورد على التنفيذ وهي خارج نطاق هذه التوصية.

R-6.4.4.4/1: يوصى أن يدعم الكيان المادي للتفتيش المتعمق على الرزمة مستوى حمولة مكونات مورد التفتيش المتعمق على الرزمة إلى مستوى الإدارة.

فعلى سبيل المثال، في الشبكات التي توجد فيها حركة اتصالات طوارئ (انظر الفقرة 1.1.7)، لا بد لعملية التفتيش المتعمق على الرزمة (DPI) من أن تكون قادرة على إعادة تسيير حركة الاتصالات في حالات الطوارئ عبر عقد ازدحام الشبكة، وبالتالي يُستحسن أن يكون نظام إدارة الشبكة عليماً بمستوى الحمل.

5.6 التفاعل مع وظيفة قرار السياسة المتبعة

R-6.5/1: يمكن اختيارياً للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يتصرف كجزء من الكيان الوظيفي لإنفاذ السياسة المتبعة على النحو المحدد في التوصية [ITU-T Y.2111]، وأن يوفر وظيفة النقل ذات الصلة.

R-6.5/2: يمكن اختيارياً للسطح البيني الذي يتوسط الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) ووظائف التحكم في الموارد والقبول (RACF) أن يكون Rw على النحو المحدد في التوصية [ITU-T Y.2111].

R-6.5/3: يمكن اختيارياً تبادل المعلومات بين الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) والكيان الوظيفي لواصف رزمة وظائف التحكم في الموارد والقبول (RACF PD-FE) عبر السطوح البينية القائمة (مثل السطح البيني *Rw*) والجديدة لهذه الوظائف حسب حالة الاستخدام المحددة للتفتيش المتعمق على الرزمة (DPI).

ملاحظـــة – في هذه الحالة، تدعو الحاجة لتعزيز وظائف التحكم في الموارد والقبول (RACF) لتشمل معلومات التفتيش المتعمق على الرزمة (DPI) (مثل توقيع البروتوكول ضمن قاعدة سياسة التفتيش المتعمق على الرزمة). فوظائف التحكم في الموارد والقبول على النحو المحدد في التوصية [ITU-T Y.2111] تدعم في المقام الأول تحديد هوية التدفق على أساس قواعد السياسة المتبعة. وتعتمد النقطة المرجعية المحددة لوظائف التحكم في الموارد والقبول على حالة الاستخدام المحددة للتفتيش المتعمق على الرزمة.

6.6 التحكم في الحركة

يمكن اشتقاق متطلبات المستوى العالي التالية:

R-6.6/1: يمكن اختيارياً للكيان الوظيفي للتفتيش المتعمق على الرزمة أن يشارك في سيناريوهات الشبكة بهدف التحكم في الحركة (على سبيل المثال، وظائف التحكم في الحركة على النحو المحدد في التوصية [ITU-T Y.1221]، ويوصى بأن يدعم الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) القدرات المقابلة للتحكم في الحركة.

R-6.6/2: يمكن اختيارياً للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يدعم أصلاً التحكم في الحركة. ومع ذلك، فإن المتطلبات التفصيلية الوظيفية للتحكم في الحركة تقع خارج نطاق هذه التوصية.

R-6.6/3: يمكن اختيارياً للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يدعم التفاعلات مع وظائف التحكم في الحركة الخارجية. وتقع المتطلبات الوظيفية ذات الصلة خارج نطاق هذه التوصية.

7.6 تحديد هوية الدورة

هناك العديد من المصطلحات المتعلقة بالدورة في هذه التوصية. ويمكن للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يحدد هوية كل حركة الدورة على نحو لا لبس فيه لأن "واصف الدورة" إما صنو لواصف التدفق و/أو التطبيق أو إنه مجموعة فرعية منه.

1.7.6 متطلبات تحديد هوية دورة

R-6.7.1/1: يجب على الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يكون قادراً على تحليل سلوك الدورة (على سبيل المثال، دورة RTP، دورة HTTP، دورة IM، دورة VoIP SIP).

R-6.7.1/2: يجب على الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يكون قادراً على تعقب حالة الدورة.

2.7.6 إجراءات التفتيش المتعمق على الرزمة (DPI) على "مستوى الدورة"

R-6.7.2/1: يمكن اختيارياً للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يستخرج أو يولد بيانات القياس على مستوى الدورة (على سبيل المثال، عن مقاييس أداء المراقبة بشأن جودة التجربة لدى المشترك).

8.6 التفتيش على الحركة المجفرة

تشيع وجهة النظر القائلة بعدم إمكانية تطبيق تواقيع التفتيش المتعمق على الرزمة (DPI) إلا على الحركة غير المجفرة. ومع ذلك، يمكن تطبيق تواقيع التفتيش المتعمق على الرزمة تبعاً لما يلي:

- مستوى التجفير (انظر الفقرة 1.8.6)
- توفر مفتاح فك التجفير محلياً (انظر الفقرة 2.8.6)
- ظروف التفتيش استناداً إلى المعلومات المجفرة (انظر الفقرة 3.8.6).

1.8.6 مدى التجفير

أي 'رزمة' بوصفها وحدة بيانات البروتوكول (PDU) تتألف معلومات التحكم في البروتوكول (PCI) ووحدات بيانات الخدمة (SDU) في مختلف طبقات البروتوكول. وعند تطبيق التجفير على مسير الاتصالات المفتَش، يمكن تطبيق التجفير:

- إما على كامل كدسة البروتوكول أو على جزء منها (الملاحظة 1)،
- ضمن طبقة البروتوكول، إما على وحدة بيانات البروتوكول (PDU) في الطبقة × (Lx) (أي Lx-PDU الكاملة) أو جزئياً فقط (على سبيل المثال، جزء معلومات التحكم في البروتوكول في الطبقة × (Lx-PCI) أو وحدات بيانات الخدمة في الطبقة × فقط (Lx-SDU)).

الملاحظـــة 1 – على سبيل المثال: يمكن لخدمة رزمة بروتوكول النقل في الوقت الفعلي (RTP) عبر بروتوكول الإنترنت (IP) أن توفر التجفير في:

أ) طبقة الشبكة (على سبيل المثال، عن طريق أسلوب نقل أمن بروتوكول الإنترنت (IPsec) أو أسلوب التمرير عبر نفق أمن بروتوكول الإنترنت)؛ و/أو

ب) طبقة النقل (على سبيل المثال، عن طريق مواصفة المستوى الأعلى الوصفية (DTLS))؛ و/أو

ج) طبقة التطبيق (على سبيل المثال، عن طريق بروتوكول الوقت الفعلي الآمن (SRTP)).

ويمكن إجراء التفتيش المتعمق على الرزمة (DPI) على أي جزء غير مجفَّر من الرزمة.

R-6.8.1/1: العلم بالحركة المجفَّرة (من منظور توقيع التفتيش المتعمق على الرزمة (DPI)): يمكن اختيارياً إجراء التفتيش المتعمق على الرزمة في جميع عناصر معلومات الحركة المفتَشة حسب مدى التجفير (الملاحظة 2).

الملاحظـــة 2 – مثال: يمكن أن يظل من الممكن تفتيش تدفق رزمة بروتوكول الوقت الفعلي الآمن (SRTP) عبر بروتوكول الإنترنت (IP) في حالة تواقيع التفتيش المتعمق على الرزمة (DPI) القائمة على عناصر معلومات التحكم في بروتوكول النقل في الوقت الفعلي (RTP PCI) ("رأسية RTP") ومعلومات التحكم في بروتوكول وحدة بيانات المستخدم (UDP PCI) ("رأسية UDP") ومعلومات التحكم في بروتوكول الإنترنت (IP PCI) ("رأسية IP") وما إلى ذلك، إذا كانت وحدات بيانات الخدمة في بروتوكول النقل في الوقت الفعلي (RTP SDU) (المتضمنة بيانات التطبيق القائم على بروتوكول الإنترنت) مجفَّرة.

R-6.8.1/2: عدم العلم بالحركة المجفَّرة (من منظور توقيع التفتيش المتعمق على الرزمة (DPI)): يمكن اختيارياً إجراء التفتيش المتعمق على الرزمة جزئياً (لأن أجزاء من تواقيع التفتيش المتعمق على الرزمة قد تكون على صلة بعناصر المعلومات غير المجفَّرة في الرزمة).

ويمكن لهذا التفتيش المتعمق الجزئي على الرزمة أن يؤدي إلى "خدمات محدودة من التفتيش المتعمق على الرزمة"، ولكنها كافية بالفعل لحالات استخدام معينة (فهي تكفي، على سبيل المثال، لتحديد الهوية تطبيق أو بروتوكول "بجزئيات تقريبية").

2.8.6 توفر مفتاح فك التجفير

R-6.8.2/1: يمكن اختيارياً تطبيق التفتيش المتعمق على الرزمة (DPI) في حال توفر مفتاح (مفاتيح) فك التجفير محلياً. وأي إنفاذ لهذا التفتيش سيعني ضمناً فك تجفير أولي (نسخة محلية) للرزمة المفتَشة.

3.8.6 شروط التفتيش القائم على معلومات مجفرة

R-6.8.3/1: يمكن اختيارياً دعم التفتيش المتعمق على الرزمة (DPI) على الحركة المجفرة في حالة شروط السياسة المتبعة السارية على عمليات التفتيش القائمة على معلومات مجفرة (ملاحظة).

ملاحظـــة – مثال: يمكن اشتقاق نمط البتات (الذي يحدد هوية تدفق رزمة معين دون لبس) برصد (تفتيش) حركة مجفرة جزئياً (انظر الفقرة 1.8.6). وستكون تواقيع التفتيش المتعمق على الرزمة (DPI) اللاحقة متوفرة سلفاً في التشفير المجفر.

4.8.6 متطلبات التفتيش المتعمق على الرزمة (DPI) الخاص بأمن بروتوكول الإنترنت (IPsec)

إن المتطلبات المذكورة في الفقرات من 1.8.6 إلى 4.8.6 تصحّ على رزم أمن بروتوكول الإنترنت المجفرة. وتركز هذه التوصية على جوانب تحديد هوية تدفق حركة أمن بروتوكول الإنترنت المجفرة. أما الجوانب المتعلقة بتحديد هوية التطبيق فتحتاج إلى مزيد من الدراسة.

1.4.8.6 المتطلبات العامة

R-6.8.4.1/1: يمكن اختيارياً للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يدعم على أقل تقدير تحديد هوية تدفق حركة أمن بروتوكول الإنترنت المجفرة. ويمكن اختيارياً لمتراتبة n من العناصر في واصف التدفق أن تنحصر في العناصر القائمة على الطبقتين L2 وL3 .

R-6.8.4.1/2: يمكن اختيارياً تقابل تدفق مع حركة ترابط أمني واحد (SA) في (IPsec)، أو يمكن اختيارياً لذلك التدفق أن يمتد عبر ترابطات أمنية متعددة.

R-6.8.4.1/3: إن تحديد هوية تدفق على أساس ترابط أمني (SA) يعني ضمناً أن مؤشر معلمة أمن بروتوكول الإنترنت (SPI) المكون من 32 بتة يمكن اختيارياً أن يكون جزءاً من واصف التدفق.

2.4.8.6 أسلوب النفق وأسلوب النقل في أمن بروتوكول الإنترنت (IPsec)

يمكن استخدام بروتوكولات أمن بروتوكول الإنترنت (رأسية الاستيقان (AH) والحمولة الأمنية المغلِّفة (ESP)، انظر أدناه) لحماية كامل حمولة بروتوكول الإنترنت (أي أسلوب النفق) أو بروتوكولات الطبقة العليا من حمولة بروتوكول الإنترنت (أي أسلوب النقل).

R-6.8.4.2/1: يمكن اختيارياً للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يكون قادراً على كشف الحركة المجفرة في أمن بروتوكول الإنترنت (IPsec) بأسلوب النفق.

R-6.8.4.2/2: يمكن اختيارياً للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يكون قادراً على كشف الحركة المجفرة في أمن بروتوكول الإنترنت (IPsec) بأسلوب النقل.

3.4.8.6 الحركة المحمية برأسية الاستيقان (AH) في أمن بروتوكول الإنترنت (IPsec)

توفر رأسية الاستيقان (AH) سلامة البيانات والاستيقان من أصل البيانات وخدمات اختيارية محدودة مضادة لتكرار الاستعراض.

R-6.8.4.3/1: يمكن اختيارياً للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يكون قادراً على كشف الحركة المحمية برأسية الاستيقان (AH) على أساس رقم بروتوكول الإنترنت المقابل لها.

4.4.8.6 الحركة المحمية بالحمولة الأمنية المغلّفة (ESP) في أمن بروتوكول الإنترنت (IPsec)

توفر الحمولة الأمنية المغلّفة (ESP) كتماناً إضافياً.

R-6.8.4.4/1: يمكن اختيارياً للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يكون قادراً على كشف الحركة المحمية بالحمولة الأمنية المغلّفة (ESP) على أساس رقم بروتوكول الإنترنت المقابل لها.

9.6 التفتيش على الحركة المضغوطة

الغرض من الضغط هو تقليل كمية الحركة. ومن الأمثلة على ذلك:

- يقلل الضغط القائم على نسق "ZIP" [b-IETF RFC 1950] من حجم الملف (فيما يتصل ببروتوكول نقل الملف (FTP) عبر تدفقات بروتوكولي TCP/IP)؛
- يقلل الضغط القائم على نسق "SigComp" [b-IETF RFC 3320] من حجم رسائل بروتوكول استهلال الدورة (SIP) (فيما يتصل ببروتوكول استهلال الدورة عبر تدفقات L4/IP).

1.9.6 طريقة العلم بالضغط

R-6.9.1/1: يمكن اختيارياً دعم التفتيش المتعمق على الرزمة عند توفر المعلومات المحلية عن خطة الضغط المطبقة (على سبيل المثال، إذا كانت عقدة التفتيش المتعمق على الرزمة على علم بأن مسير تشوير بروتوكول استهلال الدورة (SIP) المفتَش مشفَر وفق الفقرة 8 من المعيار [b-ETSI TS 124 229]). عندئذ يُستشف من أي إنفاذ للتفتيش المتعمق على الرزمة (DPI) فك ضغط أولي (لنسخة محلية) من الرزمة المفتَشة.

R-6.9.1/2: يمكن اختيارياً دعم التفتيش المتعمق على الرزمة أيضاً إذا أمكن استخلاص خطة الضغط المطبقة من تدفق الحركة المطبَقة (على سبيل المثال، يمكن اختيارياً استخلاص طريقة ضغط zip المعينة من عناصر معلومات رأسية الملف).

10.6 كشف الحركة الشاذة

1.10.6 متطلبات كشف الحركة الشاذة

R-6.10.1/1: يجب على الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يكون قادراً على دعم كشف الحركة الشاذة. وعلى وجه التحديد، يجب على تواقيع التفتيش المتعمق على الرزمة أن تكون قادرة على تشخيص الحركة الطبيعية والشاذة (على سبيل المثال، قائمة حركة سوداء أو بيضاء).

ملاحظـــة – جوانب قاعدة سياسة التفتيش المتعمق على الرزمة (DPI): قد تنطوي هذه القدرة على التحقق من العديد من المقاييس فيما يتعلق بخصائص الحركة و/أو الرزمة، فضلاً عن إمكانية استخدام شجرة قرار للتوصل إلى استنتاج نهائي بشأن أصناف الحركة الطبيعية والشاذة.

7 المتطلبات الوظيفية من منظور الشبكة

1.7 المتطلبات العامة

1.1.7 الاتصالات في حالات الطوارئ

لا بد أن يشمل مجمل تصميم وتنفيذ ونشر واستخدام وظائف التفتيش المتعمق على الرزمة (DPI) التدابير المناسبة لمنع الآثار السلبية على أداء وأمن الاتصالات في حالات الطوارئ (ET). والاتصالات في حالات الطوارئ [ITU-T Y.2205] تعني أي خدمة ذات صلة في حالات الطوارئ تتطلب معالجة خاصة بالنسبة إلى الخدمات الأخرى (على سبيل المثال، إيلاء الأولوية على الخدمات العادية). ويشمل ذلك الخدمات الحكومية المخولة في حالات الطوارئ، مثل خدمة اتصالات الطوارئ [ITU-T E.107] وخدمات السلامة العامة.

وتستند هذه التوصية إلى استخدام وسم التطبيق لتحديد الدلالات اللغوية المختلفة للتطبيقات مثل نوع بروتوكول التطبيق (على سبيل المثال، بروتوكول فيديو التوصية ITU-T H.264، أو بروتوكول استهلال الدورة (SIP) كمثال على بروتوكول تطبيق IP) وذلك بطريقة عامة. وتستخدم أنواع التطبيق نفسها (مثل SIP) لدعم الخدمات العادية وخدمات تطبيقات الاتصالات في حالات الطوارئ على السواء. بيد أن التوصية لا تفرد أي وسم تطبيق لتحديد هوية خدمات تطبيق الاتصالات في حالات الطوارئ. ولذلك، تقتضي الضرورة اتخاذ الاحتياطات المناسبة لمنع الآثار السلبية على خدمات تطبيق الاتصالات في حالات الطوارئ.

R-7.1/1: يجب عدم التدخل في إيلاء الأولوية لخدمات تطبيق الاتصالات في حالات الطوارئ على الخدمات العادية.

R-7.1/2: يجب أن يشمل مجمل تصميم وتنفيذ ونشر واستخدام وظائف التفتيش المتعمق على الرزمة (DPI) التدابير المناسبة لمنع الآثار السلبية على أداء خدمات تطبيق الاتصالات في حالات الطوارئ (مثل تأخيرها بلا داع).

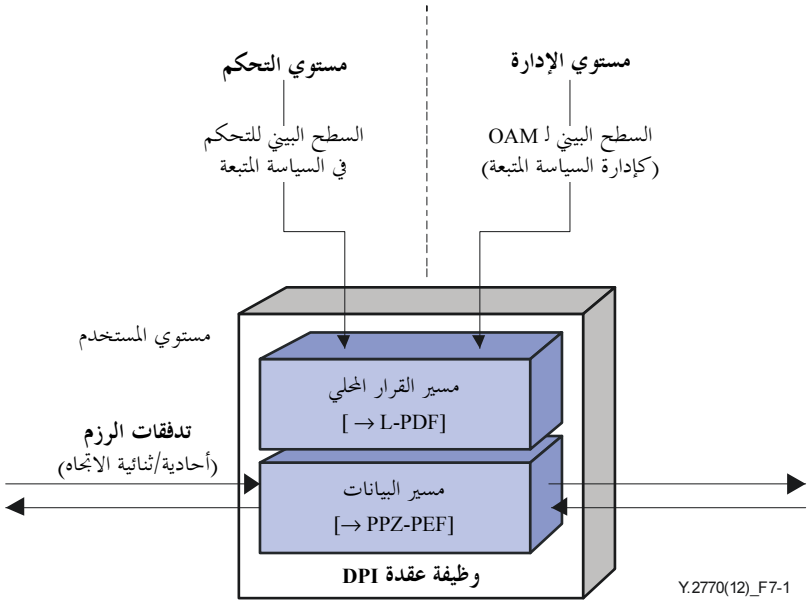
R-7.1/3: يجب أن يشمل مجمل تصميم وتنفيذ ونشر واستخدام وظائف التفتيش المتعمق على الرزمة (DPI) التدابير المناسبة لمنع ظهور ثغرات أمنية تخل بسلامة الاتصالات/الدورات في حالات الطوارئ وبسريتها وتيسرها.

ملاحظـــة – لا تضع هذه التوصية أي شروط لكيفية الوفاء بالمتطلبات المذكورة أعلاه. فقد تتحقق هذه المتطلبات من خلال استخدام القدرات الوظيفية، أو اتخاذ تدابير تشغيلية، أو بالجمع بين الأمرين كليهما.

2.7 مستوي البيانات ومستوي التحكم ومستوي الإدارة في عقدة التفتيش المتعمق على الرزمة (DPI)

1.2.7 مستويات الحركة وأنواع الحركة من منظور عقدة التفتيش المتعمق على الرزمة

تتعامل عقدة التفتيش المتعمق على الرزمة مع مسير البيانات ومسير القرار المحلي على غرار نموذج الشبكة لمستوي البيانات والتحكم والإدارة (انظر [b-ITU-T Y.2011]) (انظر الشكل 7-1). ويمكن لمسير البيانات أن يعمل بالأسلوب أحادي الاتجاه أو ثنائي الاتجاه.



الشكل 7-1 – مستويات الحركة الخارجية والداخلية في عقدة التفتيش المتعمق على الرزمة (DPI)

الملاحظـــة 1 – تسيَّر/تبدَّل تدفقات الرزمة على طول مسيرات الرزمة التي تسمى في كثير من الأحيان مسيرات البيانات في شبكات بروتوكول الإنترنت (انظر على سبيل المثال، المعيار [b-IETF RFC 4778])؛ وبالتالي فإن مصطلح مستوي البيانات مرادف لمستوي المستخدم.

الملاحظـــة 2 – يُعرف مسير بيانات بروتوكول الإنترنت بمسير وسائط بروتوكول الإنترنت (أو مسير الحمالة) في حالة حركة بيانات تطبيق بروتوكول الإنترنت، أو بمسير التشوير في حالة حركة التحكم في تطبيق بروتوكول الإنترنت [b-ITU-T X.1141].

R-7.2.1/1: يجب على عقدة التفتيش المتعمق على الرزمة (DPI) أن تدعم السطح البيني لمستوي الإدارة من أجل إدارة السياسة المتبعة ويمكنها اختيارياً أن تدعم السطح البيني لمستوي التحكم من أجل التحكم في السياسة المتبعة.

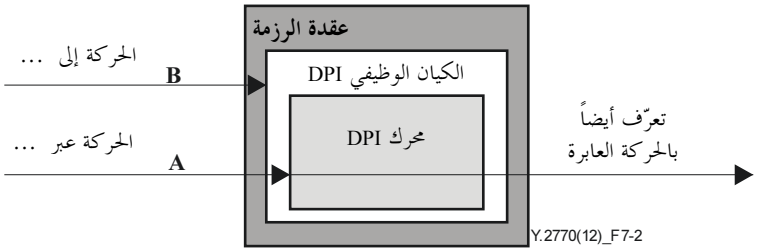
ويوفر كيان *مسير القرار المحلي* القدرات الداخلية للتحكم والإدارة في العقدة.

R-7.2.1/2: يجب على عقدة التفتيش المتعمق على الرزمة (DPI) أن تتعرف على نوعين من الرزم (انظر الشكل 7-2):

أ) رزم البيانات، التي تنتمي إلى العملاء وتحمل حركة العملاء (وتسمى "حركة **عبر**"، انظر [b-IETF opsec])؛

ب) رزم التحكم والإدارة، التي تنتمي إلى مورّد الشبكة ولها علاقة مع عمليات الشبكة (والتي تسمى "الحركة **إلى**" وانظر [b-IETF opsec]).

ويجتاز هذان النوعان من الرزم "أنبوباً مشتركاً" (فهما "ضمن النطاق")، أو يجتازان قنوات مختلفة تفرز البيانات منطقياً من رزم التحكم "من خارج النطاق" (انظر أيضاً [b-IETF RFC 4778]، الفقرة 2.2 للاطلاع على مثال على حركة الإدارة).



الشكل 7-2 – الحركة عبر (ألف) وإلى (باء) عقدة التفتيش المتعمق على الرزمة (DPI)

2.2.7 المتطلبات المتصلة بمستوي الإدارة

R-7.2.2/1: يجب على الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يدعم بروتوكولات الإدارة لإدارة تشكيلة قواعد سياسة التفتيش المتعمق على الرزمة (DPI).

R-7.2.2/2: يوصى بأن يدعم الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) إدارة معلومات هوية المستخدم والعلاقة بين المستخدم وتطبيقات المستخدم.

R-7.2.2/3: يوصى بأن يدعم الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) إدارة التطبيقات والخدمات:

- بتوليد وتعديل ونشر نماذج التطبيق؛
- وبالحفاظ على العلاقة بين التطبيقات والاستراتيجيات؛
- وبتوفير وإدارة حجز الخدمة للمستخدم.

R-7.2.2/4: يوصى بأن يدعم الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) إدارة استراتيجيات محددة سلفاً أو مولدَة دينامياً. (ويمكن اختيارياً لهذه الاستراتيجيات أن تكون على صلة بتحديد هوية التطبيق والتحكم في التطبيق وإدارة المستخدم.)

R-7.1.2/5: يوصى بأن يدعم الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) إدارة سلطة الإدارة. ولدعم الإدارة التراتبية، يتولى كل مدير سلطة إدارية مختلفة.

3.2.7 المتطلبات المتعلقة بمستوي التحكم

R-7.2.3/1: يمكن اختيارياً للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يدعم بروتوكولات التحكم في السياسة المتبعة (مثل [b-ITU-T H.248.1]) للنقطة المرجعية *Rw* لقطاع تقييس الاتصالات على النحو المعرّف في التوصية [ITU-T Y.2111]) من أجل التحكم والتشوير في قواعد سياسة التفتيش المتعمق على الرزمة (DPI).

4.2.7 المتطلبات المتعلقة بمستوي (البيانات) المستخدم

يلبي مستوي (البيانات) المستخدم المتطلبات الاختيارية التالية:

R-7.2.4/1: يمكن اختيارياً للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يدعم تكنولوجيات رزمة مختلفة (على سبيل المثال، xDSL وUMTS وCDMA2000 والكبل والشبكة المحلية (LAN) وشبكة المنطقة الواسعة (WLAN) والإثرنت وMPLS وبروتوكول الإنترنت (IP) وATM).

5.2.7 المتطلبات في كل المستويات

R-7.2.5/1: يمكن اختيارياً للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أن يدعم قواعد لغة بروتوكول موحدة لتوصيف قواعد سياسة التفتيش المتعمق على الرزمة (DPI). ويوصى على نحو محبَّذ بتطابق قواعد التركيب اللغوي في السطح البيني للتحكم في السياسة المتبعة (مستوي التحكم) وفي السطح البيني لإدارة في السياسة المتبعة (مستوي الإدارة). وهذا لا يعني ضمناً استخدام نفس البروتوكول، ولكنه يتعلق بلغة توصيف قواعد سياسة (التفتيش المتعمق على الرزمة) (وكثيراً ما تدعى لغة توصيف المرشاح (FSL) أو لغة توصيف السياسة المتبعة (PSL)؛ انظر الملاحظة).

ملاحظـــة – من أمثلة لغات البرمجة SIEVE [b-IETF RFC 5228] أو PERL أو XML أو XACML (لغة تشعبية موسعة للتحكم في النفاذ).

وتتيح قواعد لغة البروتوكول الموحدة استخدام نموذج مشترك للبيانات/الكائنات في مسير إنفاذ السياسة المتبعة ضمن عقدة التفتيش المتعمق على الرزمة (DPI)، وهو شرط مسبق لتنفيذ القاعدة على نحو فعال وسريع، فضلاً عن عمليات التحديث الخالية من الانقطاعات لمكتبة تواقيع DPI.

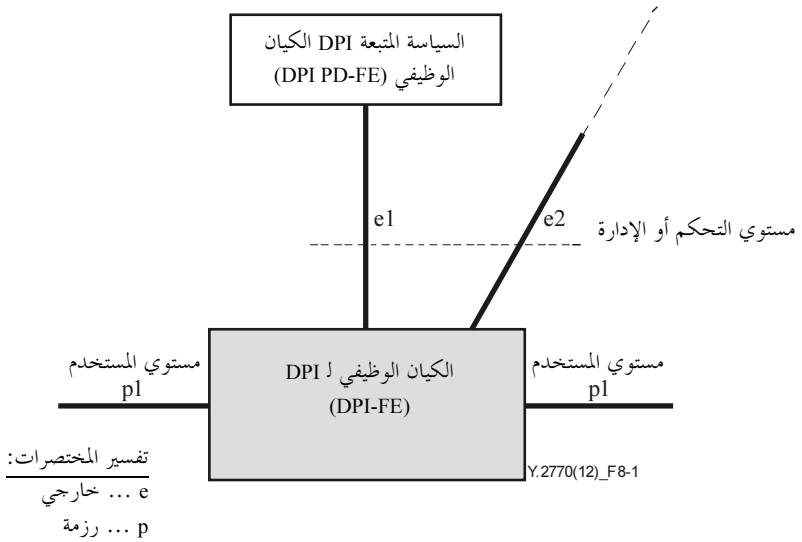
8 السطوح البينية للكيان الوظيفي للتفتيش المتعمق على الرزمة

يترتب على المتطلبات المبينة في الفقرات السابقة السطوح البينية التالية:

- ما بين الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) والكيانات الشبكية البعيدة (انظر الفقرة 1.8)،
- وما بين الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) والمكونات الداخلية (انظر الفقرة 2.8).

1.8 السطوح البينية الخارجية للكيان الوظيفي للتفتيش المتعمق على الرزمة

يصور الشكل 8-1 السطوح البينية الخارجية للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE):



الشكل 8-1 – السطوح البينية الخارجية للكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE)

1.1.8 الحركة المفتَّشة (p1)

يتبادل الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) الرزم مع عقد الرزمة البعيدة عبر السطح البيني *p1*. وطوبولوجيا مسير الرزمة هي من نقطة إلى نقطة بالنسبة إلى الكيان الوظيفي للتفتيش المتعمق على الرزمة العامل بأسلوب التفتيش المتعمق على الرزمة ضمن المسير. ولا تُدعم طبولوجيا النقاط المتعددة. ويغطي السطح البيني p1 المسيرات الثنائية الاتجاه للرزمة.

أما طوبولوجيا مسير الرزمة للكيان الوظيفي للتفتيش المتعمق على الرزمة العامل بأسلوب التفتيش المتعمق على الرزمة خارج المسير فهي على صلة بنقطة طرفية.

2.1.8 التحكم في التفتيش على الحركة وإدارته (e1)

يهدف الكيان الوظيفي المعني بقرار سياسة التفتيش المتعمق على الرزمة (DPI-PDFE) إلى التحكم في الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE) أو إدارته. ومن ثم، فإن المعلومات المتبادلة عبر السطح البيني e1 تخص أوامر التحكم في سلوك معالجة الرزمة وأوامر تشكيلها في الكيان الوظيفي للتفتيش المتعمق على الرزمة. ويمكن وصف هذه الأوامر في سياسة التفتيش المتعمق على الرزمة.

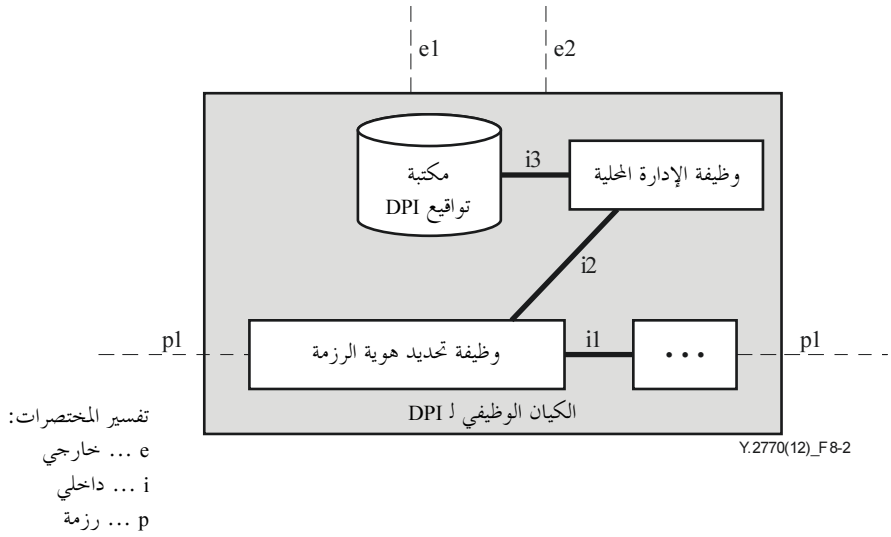
وقد يدعم السطح البيني e1 أيضاً الإبلاغ والإخطار من الكيان الوظيفي للتفتيش المتعمق على الرزمة إلى الكيان الوظيفي المعني بقرار سياسة التفتيش المتعمق على الرزمة.

3.1.8 إبلاغ الكيانات الشبكية الأخرى (e2)

يشمل السطح البيني e2 جميع السطوح البينية الممكنة للاتصالات مع الكيانات الشبكية البعيدة عدا الكيان الوظيفي المعني بقرار سياسة التفتيش المتعمق على الرزمة (DPI-PDFE). ويدعم هذا السطح البيني الإبلاغ في المقام الأول.

2.8 السطوح البينية الداخلية في الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE)

يبين الشكل 8-2 السطوح البينية الداخلية الممكنة بناءً على متطلبات التفتيش المتعمق على الرزمة (DPI):



الشكل 8-2 – السطوح البينية الداخلية في الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE)

وقد يكون هناك المزيد من المكونات الوظيفية الداخلية والسطوح البينية الداخلية في الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE). وتحتاج السطوح البينية الداخلية لمزيد من الدراسة.

3.8 متطلبات السطح البيني

R-8.3/1: يوصى بأن يتّبع السطح البيني e1 المتطلبات المذكورة في الفقرة 5.6.

R-8.3/2: يوصى بأن يتّبع السطح البيني e2 المتطلبات المذكورة في الفقرة 1.4.6.

9 اعتبارات الأمن ومتطلباته

تصف هذه الفقرة التهديدات الأمنية وتعرّف متطلبات الأمن لكيانات التفتيش المتعمق على الرزمة (DPI) في شبكات الجيل التالي.

1.9 التهديدات الأمنية ضد كيانات التفتيش المتعمق على الرزمة (DPI)

تقع عادة الكيانات الوظيفية المرتبطة بالتفتيش المتعمق على الرزمة (DPI) ضمن شبكات الجيل التالي في المنطقة الموثوقة أو المنطقة الموثوقة لكن المعرَّضة على النحو المعرَّف في التوصية [ITU-T Y.2701] التي تحدد التهديدات الأمنية لشبكات الجيل التالي وتحدد متطلبات الحماية ضد التهديدات. وبما أن الكيانات المرتبطة بالتفتيش المتعمق على الرزمة (DPI) هي جزء من شبكات الجيل التالي، تسري عليها استنتاجات التوصية [ITU-T Y.2701].وحسب هذه التوصية، تحدَد التهديدات الأمنية المتصلة بكيانات التفتيش المتعمق على الرزمة (DPI) على النحو التالي:

- تدمير المعلومات ذات الصلة بالتفتيش المتعمق على الرزمة (DPI)
- إفساد المعلومات ذات الصلة بالتفتيش المتعمق على الرزمة (DPI) أو تعديلها

- سرقة المعلومات ذات الصلة بالتفتيش المتعمق على الرزمة أو إزالتها أو فقدانها
- الإفصاح عن المعلومات ذات الصلة بالتفتيش المتعمق على الرزمة
- انقطاع الخدمات.

وتشمل المعلومات المتعلقة بعمليات التفتيش المتعمق على الرزمة (DPI) قواعد سياسة التفتيش المتعمق على الرزمة مع تواقيعها وتدفق هذا التفتيش المصدَّر ومعلومات التطبيق. ويتعذر استخدام هذه المعلومات في التفتيش المتعمق على الرزمة إذا ما تعرضت للتدمير أو الإفساد أو التعديل أو السرقة أو الإزالة أو الخسارة. وفي كثير من البلدان، يوصى بالتعامل مع مثل هذه المعلومات وفقاً لمتطلبات اللوائح والسياسات الوطنية، ويحظر الكشف عنها. قد يكون انقطاع الخدمات ناتجاً عن هجمات حجب الخدمة (DoS).

فقد تُستهدف أي جهة تتلقى بيانات بهجوم لحجب الخدمة (DoS). فعلى سبيل المثال، يستطيع مهاجم أن يغرق كيان التفتيش المتعمق على الرزمة (DPI) بحجم كبير من الحركة مما يسبب تردي خدمات التفتيش المتعمق على الرزمة أو انقطاعها عن من يحق لهم استخدامها.

2.9 متطلبات الأمن لكيانات التفتيش المتعمق على الرزمة (DPI)

فيما يلي متطلبات الأمن الأساسية لكيانات التفتيش المتعمق على الرزمة:

R-9.2/1: تجب حماية المعلومات ذات الصلة بالتفتيش المتعمق على الرزمة (DPI) الموجودة في كيانات التفتيش المتعمق على الرزمة.

R-9.2/2: إذا جرى تبادل المعلومات خارج المنطقة الموثوقة لمشغل شبكات الجيل التالي، تجب حماية المعلومات ذات الصلة بالتفتيش المتعمق على الرزمة (DPI) بين كيانات DPI والكيانات الوظيفية البعيدة (مثل DPI PD-FE وNMS).

R-9.2/3: اختيارياً أن تُستلزم آليات للتخفيف من حدة هجوم إغراق ضد الكيان الوظيفي للتفتيش المتعمق على الرزمة (DPI-FE).

R-9.2/4: يجب على منافذ البيع والمشغلين ومقدمي الخدمات أن يأخذوا في الاعتبار المتطلبات التنظيمية والسياساتية الوطنية عند تنفيذ هذه التوصية.

R-9.2/5: يُوصى بأن يستخدم المنفذون الآليات القائمة المجربة لتلبية متطلبات الأمن في هذه التوصية. على سبيل المثال، على النحو المحدد في التوصية [ITU-T Y.2704].

الملحق A

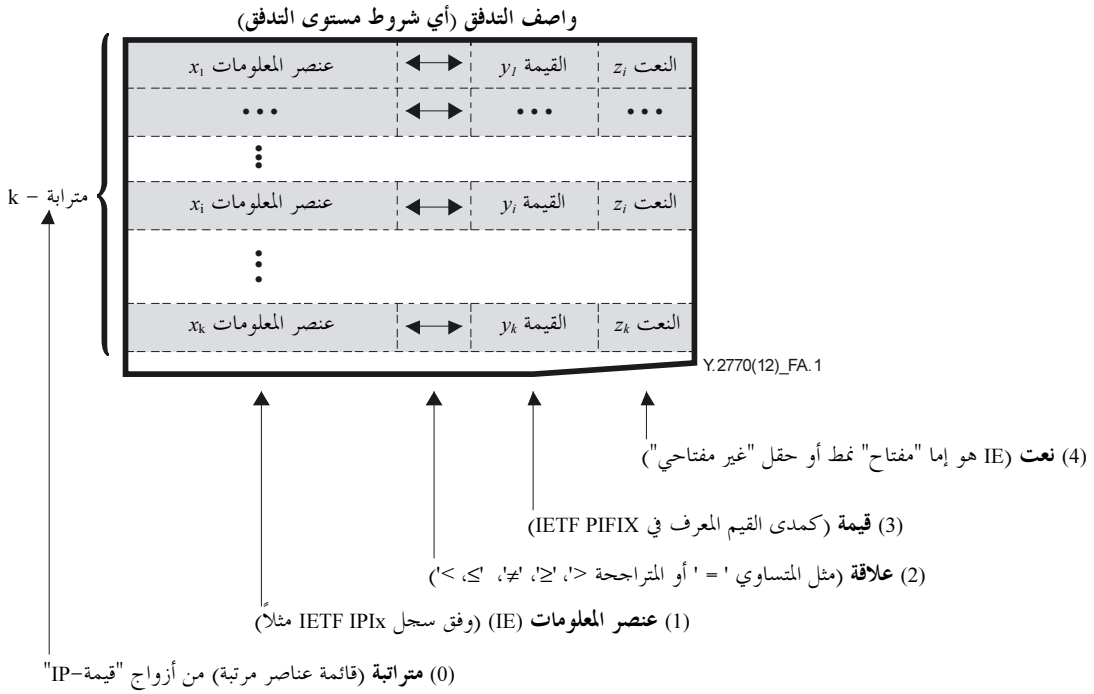
مواصفة واصف التدفق

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية)

1.A منظور التركيب اللغوي للبروتوكول

يتصل واصف التدفق *بهيكل البيانات* (كائن البيانات)، الذي يمكن نمذجته كمتراتبة عدد عناصرها k (انظر الشكل 1.A). ويتألف هيكل البيانات من عناصر معلومات (IE) عددها k (ملاحظة). وقيمة k متغيرة وهي أكبر من الصفر[1]، ولكنها ثابتة لتدفق معين. وعناصر المعلومات هي على النحو الوارد في سجل IANA IPFIX. وهناك قيمة مرتبطة بكل عنصر من عناصر المعلومات. والارتباط هو عادة المساواة الحسابية ('=')، ولكن لا تُستبعد العلاقات الرياضية الأخرى.

ملاحظـــة – يمكن أن تُنعت عناصر معلومات IETF IPFIX على أنها معلومات "حقل مفاتيح" أو "حقل غير المفاتيح".



الشكل 1.A – واصف التدفق (شروط مستوى التدفق) من منظور تركيب لغة البروتوكول

ومن ثم، يمثل واصف مستوى التدفق كمتراتبة عدد عناصرها k قائمة "أزواج اسم وقيمة" (NVP) عدد عناصرها k، وتُعرض هنا كتتابع أزواج $< IE \leftrightarrow \text{قيمة} >$[2].

---

1 ملاحظة: تشير قيمة N = 0 إلى "الاستقلالية عن التدفق".

2 على غرار هياكل أخرى مثل AVP (<اسم النعت، القيمة>)، زوج معلمة وقيمة (<معلمة=قيمة>)، إلخ.

2.A توصيف قيم عنصر المعلومات

في شروط مستوى التدفق، يمكن أن تكون قيمة عنصر المعلومات (IE):

- موصَّفة تماماً
  يمثل *التوصيف التام* حالة الإعداد الكامل للاسم والقيمة.
- أو غير موصَّفة
  تمثل القيمة *"غير الموصَّفة"* الحالة التي *لم تُسند فيها أي قيمة بعد* إلى عنصر المعلومات IE.
- أو زائدة التوصيف
  يشير *التوصيف الزائد* إلى تعدد القيم الممكنة لعنصر معلومات معين.
- أو ناقصة التوصيف
  يشير *التوصيف الناقص* إلى قيم بديلة (على سبيل المثال، جميع القيم الممكنة، أو اختيار القيمة).

3.A العلاقة بين واصف التدفق ومحدد هوية تدفق IPFIX ومفتاح تدفق IPFIX

يعرض المثال في الشكل 2.A واصف تدفق متراتبة ذات 5 عناصر يتضمن 5 مفاتيح تدفق IPFIX. ولتحديد هوية تدفق معين، يفرض واصف التدفق بعض الشروط على قيم مفاتيح التدفق هذه على النحو المحدد في الفقرة 2.A: فمفتاح التدفق الأول، IE x_1، "موصَّف تماماً"، ومفتاح التدفق الثاني، IE x_2، "زائد التوصيف"، أما عناصر المعلومات الأخرى فهي "غير موصَّفة"، على النحو المعروض في الجزء أ) من الشكل 2.A.

أ) ... تقدَّم شروط مستوى التدفق، التي يمكن أن تمثل جزئياً معلومات مفتاح تدفق IPFIX، إلى DPI-FE

واصف التدفق

IE x_1	=	موصف تماماً y_1	"مفتاح"
IE x_2	>	زائد التوصيف y_2	"مفتاح"
IE x_3		غير موصّف	"مفتاح"
IE x_4		غير موصّف	"مفتاح"
IE x_5		غير موصّف	"مفتاح"

5 مفاتيح تدفق IPFIX

ب) ... تؤدي معالجة DPI إلى تحديد هوية جميع القيم المرصودة لعناصر المعلومات (IF) ...

محدد هوية تدفق IPFIX (ملاحظة)

IE x_1	القيمة المرصودة y_1	"مفتاح"
IE x_2	القيمة المرصودة y_2	"مفتاح"
IE x_3	القيمة المرصودة y_3	"مفتاح"
IE x_4	القيمة المرصودة y_4	"مفتاح"
IE x_5	القيمة المرصودة y_5	"مفتاح"

Y.2770(12)_FA-2

ج) ... يمكن لكيان DPI-FE أخيراً أن يقدم معلومات عن التدفق الذي حُدّدت هويته (كمحدد هوية تدفق IPFEX)

t

ملاحظـــة: إن محدد هوية تدفق IPFIX هو كائن مشتق من واصف التدفق، ولذلك فهو لن يؤثر في محتوى واصف التدفق.

الشكل 2.A – مثال على واصف التدفق ومحدد هوية تدفق IPFIX ومفتاح تدفق IPFIX

لاحظ أن واصف التدفق لا يفرض شروطاً على مفاتيح تدفق IPFIX فقط: فالحال أنه في بعض الظروف قد تكن واصفات التدفق مطلوبة على غير مفتاح التدفق، على سبيل المثال، عندما يكون مطلوباً شرط أعلام بروتوكول TCP للرزمة الأولى من التدفق. والفرق الأساسي بين واصف التدفق ومحدد هوية تدفق IPFIX في مثال الشكل 2.A هو احتواء واصف التدفق على شرط "أكبر من" في مفتاح التدفق الثاني، IE x_2، (">IE x_2 قيمة y_2")، فيما يحتوي محدد هوية تدفق IPFIX القيمة المرصودة لمفتاح التدفق الثاني، IE x_2، أي القيمة yy_2. ويتكون محدد هوية تدفق IPFIX من مجموعة من القيم المرصودة لمفاتيح التدفق، حالما يقوم الكيان الوظيفي للتفتيش المتعمق على الرزمة بمعالجة الرزم وتصنيفها ضمن تدفق ما.

ولاحظ أنه إذا تضمنت المعلومات المصدَّرة (مثلاً عبر سجل تدفق IPFIX) كل من عناصر المعلومات إلى جانب مع القيم المرصودة المرتبطة بها، وبصرف النظر عما إذا كان عنصر المعلومات عائداً لمفتاح تدفق IPFIX أم لا، لا حاجة لتخصيص محدد هوية موصَّف لتدفق IPFIX، لأن محدد هوية تدفق IPFIX هو مجموع كل هذه المعلومات.

بيبليوغرافيا

[b-ITU-T H.248.1] Recommendation ITU-T H.248.1 v3 (2005), *Gateway Control Protocol: Version 3*.

[b-ITU-T X.734] Recommendation ITU-T X.734 (1992), *Information technology – Open Systems Interconnection – Systems Management: Event report management function*.

[b-ITU-T X.1141] Recommendation ITU-T X.1141 (2006), *Security Assertion Markup Language (SAML 2.0)*.

[b-ITU-T Y.2011] Recommendation ITU-T Y.2011 (2004), *General principles and general reference model for Next Generation Networks*.

[b-ITU-T Y.2121] Recommendation ITU-T Y.2121 (2008), *Requirements for the support of flow-state-aware transport technology in NGN*.

[b-ETSI ES 282 003] ETSI ES 282 003 (2011), *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture*.

[b-ETSI TS 123 203] ETSI TS 123 203 (2011), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Policy and charging control architecture (3GPP TS 23.203 version 10.4.0 Release 10)*.

[b-ETSI TS 124 229] ETSI TS 124 229 (2009), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE;IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229 version 9.4.0 Release 9)*.

[b-IETF IANA IPFIX] IETF IANA IPFIX (2007), IP Flow Information Export (IPFIX) Entities. <http://www.iana.org/assignments/ipfix/ipfix.xhtml>

[b-IETF opsec] IETF draft-ietf-opsec-filter-caps (2007), *Filtering and Rate Limiting Capabilities for IP Network Infrastructure*. <http://tools.ietf.org/html/draft-ietf-opsec-filter-caps-09>

[b-IETF RFC 1950] IETF RFC 1950 (1996), *ZLIB Compressed Data Format Specification version 3.3*.

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

[b-IETF RFC 3320] IETF RFC 3320 (2003), *Signaling Compression (SigComp)*.

[b-IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

[b-IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol*.

[b-IETF RFC 3871] IETF RFC 3871 (2004), *Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure*.

[b-IETF RFC 4268] IETF RFC 4268 (2005), *Entity State MIB*.

[b-IETF RFC 4778] IETF RFC 4778 (2007), *Operational Security Current Practices in Internet Service Provider Environments*.

[b-IETF RFC 4867] IETF RFC 4867 (2007), *RTP Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs*.

[b-IETF RFC 5102] IETF RFC 5102 (2008), *Information Model for IP Flow Information Export*.

[b-IETF RFC 5103] IETF RFC 5103 (2008), *Bidirectional Flow Export Using IP Flow Information Export (IPFIX)*.

[b-IETF RFC 5228] IETF RFC 5228 (2008), *Sieve: An Email Filtering Language*.

[b-IETF RFC 5424] IETF RFC 5424 (2009), *The Syslog Protocol*.

[b-IETF RFC 5426] IETF RFC 5426 (2009), *Transmission of Syslog Messages over UDP*.

[b-IETF RFC 5476] IETF RFC 5476 (2009), *Packet Sampling (PSAMP) Protocol Specifications*.

[b-PacketTypes] McCann, P.J., and Chandra S. (2000), *Packet Types: Abstract Specification of Network Protocol Messages*; in SIGCOMM '00: Proceedings of the conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, pp. 321-333, ACM Press, New York.

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	المطاريف وطرائق التقييم الذاتية والموضوعية
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التلماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن
السلسلة Y	**البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي**
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2014