الاتحـــــــــــاد الدولـــــــــــي للاتصـــــــــــالات

ITU-T

قطاع تقييس الاتصالات
في الاتحاد الدولي للاتصالات

X.1042

(2019/01)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

أمن المعلومات والشبكات – أمن الشبكة

خدمات الأمن باستخدام التوصيل الشبكي المعرَّف بالبرمجيات

التوصية ITU-T X.1042

الاتحاد الدولي للاتصالات

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.1–X.199
التوصيل البيني للأنظمة المفتوحة	X.200–X.299
التشغيل البيني للشبكات	X.300–X.399
أنظمة معالجة الرسائل	X.400–X.499
الدليل	X.500–X.599
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.600–X.699
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.700–X.799
الأمن	X.800–X.849
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.850–X.899
المعالجة الموزعة المفتوحة	X.900–X.999
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1000–X.1029
أمن الشبكة	**X.1030–X.1049**
إدارة الأمن	X.1050–X.1069
الخصائص البيومترية	X.1080–X.1099
تطبيقات وخدمات آمنة (1)	
أمن البث المتعدد	X.1100–X.1109
أمن الشبكة المحلية	X.1110–X.1119
أمن الخدمات المتنقلة	X.1120–X.1139
أمن الويب	X.1140–X.1149
بروتوكولات الأمن (1)	X.1150–X.1159
الأمن بين جهتين نظيرتين	X.1160–X.1169
أمن معرفات الهوية عبر الشبكات	X.1170–X.1179
أمن التلفزيون القائم على بروتوكول الإنترنت	X.1180–X.1199
أمن الفضاء السيبراني	
الأمن السيبراني	X.1200–X.1229
مكافحة الرسائل الاقتحامية	X.1230–X.1249
إدارة الهوية	X.1250–X.1279
تطبيقات وخدمات آمنة (2)	
اتصالات الطوارئ	X.1300–X.1309
أمن شبكات المحاسيس واسعة الانتشار	X.1310–X.1319
أمن شبكة الكهرباء الذكية	X.1330–X.1339
البريد المعتمد	X.1340–X.1349
أمن إنترنت الأشياء (IoT)	X.1360–X.1369
أمن أنظمة النقل الذكية (ITS)	X.1370–X.1389
أمن سجل الحسابات الموزع	X.1400–X.1429
البروتوكول الأمني (2)	X.1450–X.1459
تبادل معلومات الأمن السيبراني	
نظرة عامة عن الأمن السيبراني	X.1500–X.1519
تبادل مواطن الضعف/الحالة	X.1520–X.1539
تبادل الأحداث/الأحداث العارضة/المعلومات الحدسية	X.1540–X.1549
تبادل السياسات	X.1550–X.1559
طلب المعلومات الحدسية والمعلومات الأخرى	X.1560–X.1569
تعرف الهوية والاكتشاف	X.1570–X.1579
التبادل المضمون	X.1580–X.1589
أمن الحوسبة السحابية	
نظرة عامة على أمن الحوسبة السحابية	X.1600–X.1601
تصميم أمن الحوسبة السحابية	X.1602–X.1639
أفضل الممارسات ومبادئ توجيهية بشأن أمن الحوسبة السحابية	X.1640–X.1659
تنفيذ أمن الحوسبة السحابية	X.1660–X.1679
أمن أشكال أخرى للحوسبة السحابية	X.1680–X.1699

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

التوصية ITU-T X.1042

خدمات الأمن باستخدام التوصيل الشبكي المعرَّف بالبرمجيات

ملخص

تدعم التوصية ITU-T X.1042 حماية موارد الشبكة باستخدام خدمات الأمن القائمة على التوصيل الشبكي المعرَّف بالبرمجيات (SDN). وتصنف هذه التوصية أولاً موارد الشبكة لخدمات الأمن القائمة على التوصيل الشبكي المعرَّف بالبرمجيات وهي: تطبيق التوصيل الشبكي المعرَّف بالبرمجيات، ووحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات، وبدالة التوصيل الشبكي المعرَّف بالبرمجيات ومدير أمن (SM) التوصيل الشبكي المعرَّف بالبرمجيات. ثم تعرِّف هذه التوصية خدمات الأمن القائمة على التوصيل الشبكي المعرَّف بالبرمجيات.

التسلسل التاريخي

الطبعة	التوصية	تاريخ الموافقة	لجنة الدراسات	معرف الهوية الفريد*
1.0	ITU-T X.1042	2019-01-30	17	11.1002/1000/13803

مصطلحات أساسية

التحكم في النفاذ، هجوم حرمان من الخدمة موزَّع (DDoS)، جدار الحماية، مصيدة جاذبة، التوصيل الشبكي المعرَّف بالبرمجيات (SDN)، سيناريوهات الأمن.

* للنفاذ إلى توصية، ترجى كتابة العنوان http://handle.itu.int/ في حقل العنوان في متصفح الويب لديكم، متبوعاً بمعرف التوصية الفريد. ومثال ذلك، http://handle.itu.int/11.1002/1000/11830-en.

تمهيد

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 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

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

ملاحظة

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 البيانات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

© ITU 2019

جميع الحقوق محفوظة. لا يجوز استنساخ أي جزء من هذه المنشورة بأي وسيلة كانت إلا بإذن خطي مسبق من الاتحاد الدولي للاتصالات.

جدول المحتويات

الصفحة

مشروع التوصية ITU-T X.1042

خدمات الأمن باستخدام التوصيل الشبكي المعرَّف بالبرمجيات

1 مجال التطبيق

تدعم هذه التوصية حماية موارد الشبكة باستخدام خدمات الأمن القائمة على التوصيل الشبكي المعرَّف بالبرمجيات (SDN). وتغطي هذه التوصية ما يلي:

- تصنيف موارد الشبكة التي يمكن أن تحميها خدمات الأمن القائمة على التوصيل الشبكي المعرَّف بالبرمجيات؛
- تعريف خدمات الأمن القائمة على التوصيل الشبكي المعرَّف بالبرمجيات؛
- توصيف تنفيذ خدمات الأمن القائمة على التوصيل الشبكي المعرَّف بالبرمجيات.

إن حماية موارد الشبكة (من قبيل المسيِّر، والبدالة، وجدار الحماية، ونظام كشف التسلل) بواسطة خدمات الأمن على التوصيل الشبكي المعرَّف بالبرمجيات تعني ما يلي:

- رد فوري على هجمات جديدة على الشبكة (مثل هجمات الديدان البرمجية وهجمات DDoS)؛
- بناء شبكات خاصة للتخفيف من هجمات ماكرة على الشبكة؛
- الدفاع التلقائي ضد هجمات على الشبكة دون تدخل من مسؤولي الشبكة؛
- توزيع الموارد المواكب للحمولة الدينامية للشبكة.

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، يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T Y.3300] التوصية ITU-T Y.3300 (2014)، *إطار للتوصيل الشبكي المعرف بالبرمجيات.*

[ITU-T Y.3301] التوصية ITU-T Y.3301 (2016)، *المتطلبات الوظيفية للتوصيل الشبكي المعرف بالبرمجيات.*

[ITU-T Y.3302] التوصية ITU-T Y.3302 (2017)، *المعمارية الوظيفية للتوصيل الشبكي المعرف بالبرمجيات.*

3 التعاريف

1.3 المصطلحات المعرَّفة في مراجع أخرى

تستخدم هذه التوصية المصطلحات التالية المعرَّفة في مراجع أخرى:

1.1.3 التوصيل الشبكي المعرّف بالبرمجيات (software-defined networking) [ITU-T Y.3300]: مجموعة من التقنيات تمكن من برمجة موارد الشبكة وضبط إيقاعها والتحكم فيها وإدارتها مباشرة، مما يسهل تصميم خدمات الشبكة وتسليمها وتشغيلها بطريقة دينامية وقابلة للتوسعة.

2.1.3 التحكم في النفاذ (access control) [b-ITU-T X.1252]: إجراء متبع لتحديد ما إذا كان ينبغي منح كيان ما نفاذاً إلى موارد أو مرافق أو خدمات أو معلومات استناداً إلى ما هو محدد مسبقاً من قواعد وحقوق معينة أو إلى سلطة يتمتع بها الطرف الطالب.

3.1.3 سياسة التحكم في النفاذ (access control policy) [b-ITU-T X.812]: مجموعة القواعد التي تحدد الشروط التي يمكن أن يحدث بموجبها النفاذ.

4.1.3 قواعد سياسة التحكم في النفاذ (access control policy rules) [b-ITU-T X.812]: قواعد السياسة الأمنية المتعلقة بتقديم خدمة التحكم في النفاذ.

2.3 المصطلحات المعرَّفة في هذه التوصية

تعرِّف هذه التوصية المصطلحات التالية:

1.2.3 مورد الشبكة (network resource): جهاز يقوم بإعادة تسيير الرزمة في نظام شبكة.

ملاحظة – تشتمل موارد الشبكة على بدالات الشبكة والمسيِّرات والبوابات ونقاط النفاذ عبر WiFi.

2.2.3 جدار الحماية (firewall): جهاز أو خدمة عند ملتقى قطاعين في الشبكة يتفحص كل رزمة تحاول عبور الحدود. ويرفض أيضاً أي رزمة مستبعَدة بمعايير معينة مثل وجود أرقام المنافذ أو عناوين بروتوكول الإنترنت (IP) غير المسموح بها.

ملاحظة – يمكن فصل خدمات جدار الحماية عن الأجهزة المادية وتشغيلها كتطبيق.

3.2.3 المصيدة الجاذبة (honeypot): آلية أمن حاسوبي تُنصَب كشرك لجذب المهاجمين السيبرانيين. وهي تُستخدم لكشف الهجمات أو إبعادها عن هدف مشروع ولجمع بيانات الهجوم. ومصطلح المصيدة الجاذبة أو honeypot بالإنكليزية الذي يعني كوز العسل حرفياً هو مصطلح مشتق من سلوكه الذي يجذب المهاجمين ("النحل") إلى مكان (هدف الهجوم، أو "العسل")، أي أنه يُستخدم كمصيدة.

4.2.3 خدمة جدار الحماية المركزية (centralized firewall service): خدمة يمكنها إنشاء وتوزيع قواعد سياسة التحكم في النفاذ إلى موارد الشبكة من أجل كفاءة إدارة جدار الحماية. وتمكن إدارة هذه القواعد بشكل دينامي من خلال مخدِّم مركزي. ويمكن أن يعمل التوصيل الشبكي المعرَّف بالبرمجيات (SDN) كخدمة جدار حماية مركزية عبر سطح بيني معياري بين تطبيقات جدار الحماية وموارد الشبكة.

5.2.3 خدمة تخفيف هجمات DDoS المركزية (centralized DDoS-attack mitigation service): خدمة يمكنها إنشاء وتوزيع قواعد سياسة التحكم في النفاذ إلى موارد الشبكة من أجل كفاءة تخفيف هجمات الحرمان من الخدمة الموزَّعة (DDoS). وتمكن إدارة هذه القواعد بشكل دينامي من خلال مخدِّم مركزي. ويمكن أن يعمل التوصيل الشبكي المعرَّف بالبرمجيات (SDN) كخدمة تخفيف هجمات DDoS مركزية عبر سطح بيني معياري بين تطبيقات تخفيف هجمات DDoS وموارد الشبكة.

6.2.3 خدمة المصيدة الجاذبة المركزية (centralized honeypot service): خدمة يمكنها إنشاء وتوزيع قواعد سياسة التحكم في النفاذ إلى موارد الشبكة لتشكيل مصيدة جاذبة دينامية. وتمكن إدارة هذه القواعد بشكل دينامي من خلال مخدِّم مركزي. ويمكن أن يعمل التوصيل الشبكي المعرَّف بالبرمجيات (SDN) كخدمة مصيدة جاذبة مركزية عبر سطح بيني معياري بين تطبيقات المصيدة الجاذبة وموارد الشبكة.

7.2.3 خدمة الإدارة المركزية للأجهزة غير القانونية (centralized illegal device management service): خدمة يمكنها إنشاء وتوزيع قواعد سياسة التحكم في النفاذ إلى موارد الشبكة بشأن القائمة السوداء للأجهزة غير القانونية. ويمكن إدارة هذه القواعد بشكل دينامي وعالمي من خلال مخدِّم مركزي. ويمكن أن يعمل التوصيل الشبكي المعرَّف بالبرمجيات (SDN) كإدارة لأجهزة غير قانونية تستند إلى الشبكة عبر سطح بيني معياري بين تطبيقات إدارة الأجهزة غير القانونية وموارد الشبكة.

الملاحظة – إن قاعدة اتخاذ قرار بشأن جهاز غير قانوني تقع خارج مجال تطبيق هذه التوصية. ويمكن أن يتحدد مثال على الجهاز غير القانوني وفقاً لاستخدام نظام التعريف الفريد العالمي.

8.2.3 خدمة إدارة التحكم في النفاذ: خدمة يمكنها وضع وتوزيع سياسات حقوق نفاذ القائمة البيضاء بأجهزة إنترنت الأشياء (IoT) إلى موارد الشبكة. وتمكن إدارة هذه القواعد بشكل دينامي وعالمي من خلال مخدِّم مركزي. ويمكن أن يعمل التوصيل الشبكي المعرَّف بالبرمجيات (SDN) كإدارة لأجهزة إنترنت الأشياء تستند إلى الشبكة عبر سطح بيني معياري بين تطبيقات إدارة التحكم في النفاذ وموارد الشبكة.

ملاحظة – يقع توصيف التكوين التراتبي لسياسات النفاذ خارج مجال تطبيق هذه التوصية. ويمكن تكوين سياسات النفاذ هذه وتقسيمها وفقاً لمستوى أمن موارد الشبكة وتوزيعها على نظام الشبكة.

4 المختصرات والأسماء المختصرة

تستخدم هذه التوصية المختصرات التالية:

ACI السطح البيني للتحكم في التطبيق *(Application Control Interface)*

ACM إدارة التحكم في النفاذ *(Access Control Management)*

AL-MSO دعم وضبط إيقاع إدارة طبقة التطبيق *(Application Layer Management Support and Orchestration)*

ALM إدارة طبقة تطبيق *(Application Layer Management)*

BSS نظام دعم الأعمال *(Business Support System)*

CL-AS دعم تطبيق طبقة التحكم (Control Layer Application Support)

CL-CLS خدمة طبقة التحكم في طبقة التحكم *(Control Layer Control Layer Service)*

CL-MSO دعم وضبط إيقاع إدارة طبقة التحكم *(Control Layer Management Support and Orchestration)*

CL-RA تجريد موارد طبقة التحكم *(Control Layer Resource Abstraction)*

CLM إدارة طبقة التحكم *(Control Layer Management)*

DDoS الحرمان من الخدمة الموزَّع *(Distributed Denial-of-Service)*

DNS خدمة اسم الميدان *(Domain Name Service)*

DPI تفحص الرزم المعمق *(Deep Packet Inspection)*

I2NSF السطح البيني مع وظيفة أمن الشبكة *(Interface to Network Security Function)*

IoT إنترنت الأشياء *(Internet of Things)*

IP بروتوكول الإنترنت *(Internet Protocol)*

MAC تحكم في النفاذ إلى الوسائط *(Media Access Control)*

MMF وظيفة إدارة متعددة الطبقات *(Multi-layer Management Function)*

MMFA طبقة التطبيق في وظيفة إدارة متعددة الطبقات *(Multi-layer Management Function Application layer)*

MMFC طبقة التحكم في وظيفة إدارة متعددة الطبقات *(Multi-layer Management Function Control layer)*

MMFO وظيفة إدارة متعددة الطبقات OSS/BSS *(Multi-layer Management Functions OSS/BSS)*

MMFR طبقة الموارد في وظيفة إدارة متعددة الطبقات *(Multi-layer Management Function Resource layer)*

NSF وظيفة أمن الشبكة *(Network Security Function)*

OSS نظام دعم التشغيل *(Operation Support System)*

RCI السطح البيني للتحكم في الموارد *(Resource Control Interface)*

RLM إدارة طبقة الموارد *(Resource Layer Management)*

RL-MS دعم إدارة طبقة الموارد *(Resource Layer Management Support)*

SDN التوصيل الشبكي المعرَّف بالبرمجيات *(Software-Defined Networking)*

SDN-AL طبقة التطبيق في التوصيل الشبكي المعرَّف بالبرمجيات *(Software-Defined Networking - Application Layer)*

SDN-CL طبقة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات *(Software-Defined Networking - Control Layer)*

SDN-RL طبقة الموارد في التوصيل الشبكي المعرَّف بالبرمجيات *(Software-Defined Networking - Resource Layer)*

SIP بروتوكول استهلال الدورة *(Session Initiation Protocol)*

SM مدير الأمن *(Security Manager)*

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

VoIP الاتصالات الصوتية عبر بروتوكول الإنترنت *(Voice over Internet Protocol)*

VoLTE الاتصالات الصوتية عبر التطور الطويل الأجل *(Voice over Long-Term Evolution)*

5 الاصطلاحات

يتعين فهم المصطلحات الأساسية التالية في هذه التوصية على النحو التالي:

"يتعين" تدل على متطلَّب إلزامي يجب التقيّد به بصرامة، ولا يُسمح بأي انحراف عنه في حال ادعاء الامتثال لهذه التوصية.

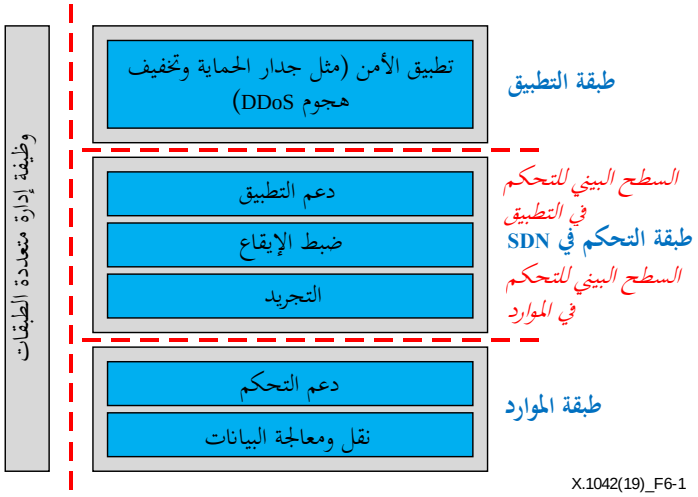
"يوصى" كلمة تدل على متطلب يوصى به لكنه غير إلزامي بالمطلق. وبالتالي لا يتعين تقدم هذا المتطلب لزعم الامتثال.

"يحظر" تدل على متطلب إلزامي يجب التقيد به بصرامة ولا يسمح بأي انحراف عنه في حال زعم الامتثال لهذه التوصية.

"من الجائز": تدل على مطلب اختياري مسموح به دون أن ينطوي على أي توصية به. ولا يرمي هذا المصطلح إلى إلزام تطبيق البائع بتقديم هذا الخيار الذي يمكن أن يقدمه مشغل الشبكة/مورد الخدمة اختيارياً. وبالأحرى، فإن البائع يمكنه إدراج هذه الخاصية اختيارياً ويدعى إلى الامتثال لهذه المواصفة في نفس الوقت.

6 نظرة عامة على المعمارية الوظيفية للتوصيل الشبكي المعرَّف بالبرمجيات (SDN)

تصف هذه الفقرة المعمارية المرجعية الإجمالية لخدمات الأمن (مثل جدار الحماية وتخفيف هجوم DDoS) باستخدام المعمارية الإجمالية للتوصيل الشبكي المعرَّف بالبرمجيات في التوصية [ITU-T Y.3300]، من قبيل خدمة جدار الحماية المركزية وخدمة تخفيف هجوم DDoS المركزية.



الشكل 6-1 – المعمارية الإجمالية لخدمات الأمن القائمة على التوصيل الشبكي المعرَّف بالبرمجيات (SDN)

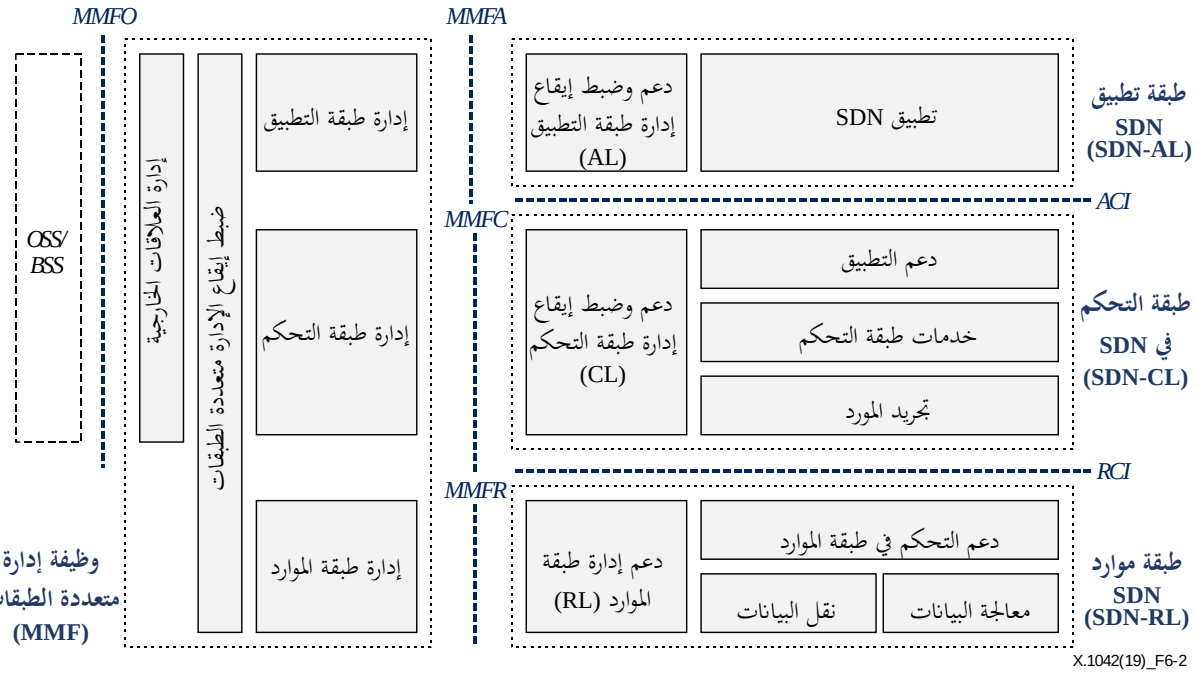
على النحو المبين في الشكل 6-1، تشغِّل التطبيقات الخاصة بخدمات الأمن (مثل خدمات جدار الحماية وتخفيف هجوم DDoS والمصيدة الجاذبة) تعمل فوق معمارية التوصيل الشبكي المعرَّف بالبرمجيات (SDN). وعندما يقوم مستخدم أو مسؤول (إدارة طبقة التطبيق (ALM) في الشكل 6-2 مثلاً) بإنفاذ سياسات أمن لخدمات الأمن من خلال سطح بيني للتطبيق، تقوم وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) بإنشاء قواعد التحكم في النفاذ المقابلة للإيفاء بمثل هذه السياسات الأمنية بطريقة مستقلة وفورية. ووفقاً لقواعد التحكم في النفاذ، تقوم موارد الشبكة المتولدة مثل بدالات التوصيل الشبكي المعرَّف بالبرمجيات (SDN) بالتصرف للتخفيف من الهجمات على الشبكة، من قبيل إسقاط الرزم ذات الأنماط المشبوهة.

ويبين الشكل 6-2 المعمارية الوظيفية للتوصيل الشبكي المعرَّف بالبرمجيات في التوصية [ITU-T Y.3302]، التي تستند إلى المعمارية الإجمالية للتوصيل الشبكي المعرَّف بالبرمجيات.

- طبقة تطبيق التوصيل الشبكي المعرَّف بالبرمجيات (SDN-AL): تتألف طبقة تطبيق التوصيل الشبكي المعرَّف بالبرمجيات من المكون الوظيفي لدعم وضبط إيقاع إدارة طبقة التطبيق (AL-MSO) والمكونات الوظيفية المتعددة لتطبيق التوصيل الشبكي المعرَّف بالبرمجيات [ITU-T Y.3302]. ويتفاعل AL-MSO مع المكون الوظيفي لإدارة طبقة التطبيق (ALM) في وظيفة الإدارة متعددة الطبقات (MMF) عبر النقطة المرجعية لطبقة تطبيق وظيفة الإدارة متعددة الطبقات (MMFA) من أجل دعم إدارة تطبيقات التوصيل الشبكي المعرَّف بالبرمجيات (SDN) وتمكين التشغيلات المشتركة للإدارة في جميع طبقات SDN الفرعية. وتتفاعل تطبيقات SDN مع طبقة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN-CL) عبر النقطة المرجعية للسطح البيني للتحكم في التطبيق (ACI) مع طلبات SDN-CL لتفصيل سلوك وخصائص موارد الشبكة تلقائياً على مقاس الطلبات. وتستخدم تطبيقات التوصيل الشبكي المعرَّف بالبرمجيات (SDN) المشهد المجرد وحالة موارد الشبكة التي تقدمها طبقة SDN-CL عن طريق نماذج المعلومات والبيانات المكشوفة عبر النقطة المرجعية للسطح البيني للتحكم في التطبيق (ACI). وحسب حالات استخدام التوصيل الشبكي المعرَّف بالبرمجيات (SDN) (على سبيل المثال، داخل مراكز البيانات أو فيما بينها، أو شبكات الاتصالات المتنقلة، أو شبكات النفاذ)، يمكن تحديد السطوح البينية للتحكم في التطبيق بشكل اختياري. ويُفترض أن تُستخدم هذه السطوح البينية كسطوح بينية لبرمجة التطبيقات (API) المفتوحة.
- طبقة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN-CL): تتكون SDN-CL من دعم وضبط إيقاع إدارة طبقة التحكم (CL-MSO)، ودعم تطبيق طبقة التحكم (CL-AS)، وخدمات طبقة التحكم في طبقة التحكم (CL-CLS)، وتجريد الموارد (CL-RA). وتقدم طبقة SDN-CL وسائل قابلة للبرمجة للتحكم في سلوك موارد SDN (مثل موارد نقل ومعالجة البيانات)، وفقاً لطلبات طبقة SDN-AL وسياسات وظيفة MMF. وتعمل طبقة SDN-CL على الموارد التي تقدمها طبقة موارد SDN (SDN-RL) وتكشف لطبقة SDN-AL مشهداً مجرداً عن الشبكة. وتتفاعل طبقة SDN-CL مع طبقة SDN-RL باستخدام نقطة مرجعية للسطح البيني للتحكم في الموارد (RCI)، مع مكون وظيفي لإدارة طبقة

التحكم (CLM) في وظيفة MMF باستخدام النقطة المرجعية لطبقة التحكم في وظيفة إدارة متعددة الطبقات (MMFC). وهي تتفاعل أيضاً مع طبقة SDN-AL بواسطة النقطة المرجعية للسطح البيني للتحكم في التطبيق (ACI). ويمكن أن يطلب دعم وضبط إيقاع إدارة طبقة التحكم (CL-MSO) من وظيفة MMF تفويض بعض وظائف الإدارة. فتقدم وظيفة MMF خواصاً وظيفية لإدارة الخواص الوظيفية لطبقة SDN-CL من خلال النقطة المرجعية لوظيفة MMFC.

– طبقة موارد التوصيل الشبكي المعرَّف بالبرمجيات (SDN-RL): تتألف طبقة SDN-RL من دعم إدارة طبقة الموارد (RL-MS)، ودعم التحكم في طبقة الموارد، ومعالجة بيانات طبقة الموارد، ونقل بيانات طبقة الموارد. وطبقة SDN-RL هي المكان الذي تقوم فيه عناصر الشبكة المادية أو الافتراضية بإجراء نقل و/أو معالجة رزم البيانات وفقاً لقرارات طبقة SDN-CL. ويجري تبادل معلومات التهيئة للسياسة المتبعة (بما في ذلك معلومات التشكيلة) التي تنتج عن القرارات التي تتخذها طبقة SDN-CL وكذلك المعلومات عن موارد الشبكة عبر النقطة المرجعية للسطح البيني للتحكم في الموارد (RCI). وتتضمن المعلومات المتبادلة من خلال السطح البيني للتحكم في الموارد معلومات التحكم المقدمة من طبقة SDN-CL إلى طبقة SDN-RL (لتشكيل مورد شبكة أو تقديم سياسات على سبيل المثال) بالإضافة إلى المعلومات المتعلقة بالتبليغات المرسَلة من طبقة SDN-RL عند كشف تغيير مورد الشبكة (إذا كانت هذه المعلومات متاحة). ويقدم دعم إدارة طبقة الموارد (RL-MS) وصفاً للمورد، أي المورِّد ونسخة البرمجيات وحالتها (من قبيل حمولة وحدة المعالجة المركزية أو ذاكرة النفاذ العشوائي (RAM) المستخدمة أو التخزين). وقد يتضمن وكيل إدارة يقوم ببعض عمليات الإدارة المحلية في حال تفويضه من وظيفة MMF. وتقدم وظيفة الإدارة متعددة الطبقات (MMF) خواص وظيفية لإدارة الخواص الوظيفية لطبقة SDN-RL من خلال النقطة المرجعية لطبقة الموارد في وظيفة إدارة متعددة الطبقات (MMFR).



BSS: نظام دعم الأعمال؛ MMFO: وظيفة إدارة متعددة الطبقات OSS/BSS؛ OSS: نظام دعم التشغيل

الشكل 6-2 – المعمارية الوظيفية للتوصيل الشبكي المعرَّف بالبرمجيات (SDN) [ITU-T Y.3302]

7 تصنيف موارد الشبكة

تعرِّف هذه الفقرة أربعة موارد شبكة لخدمات الأمن باستخدام التوصيل الشبكي المعرَّف بالبرمجيات (SDN) بناءً على الشكل 6-2:

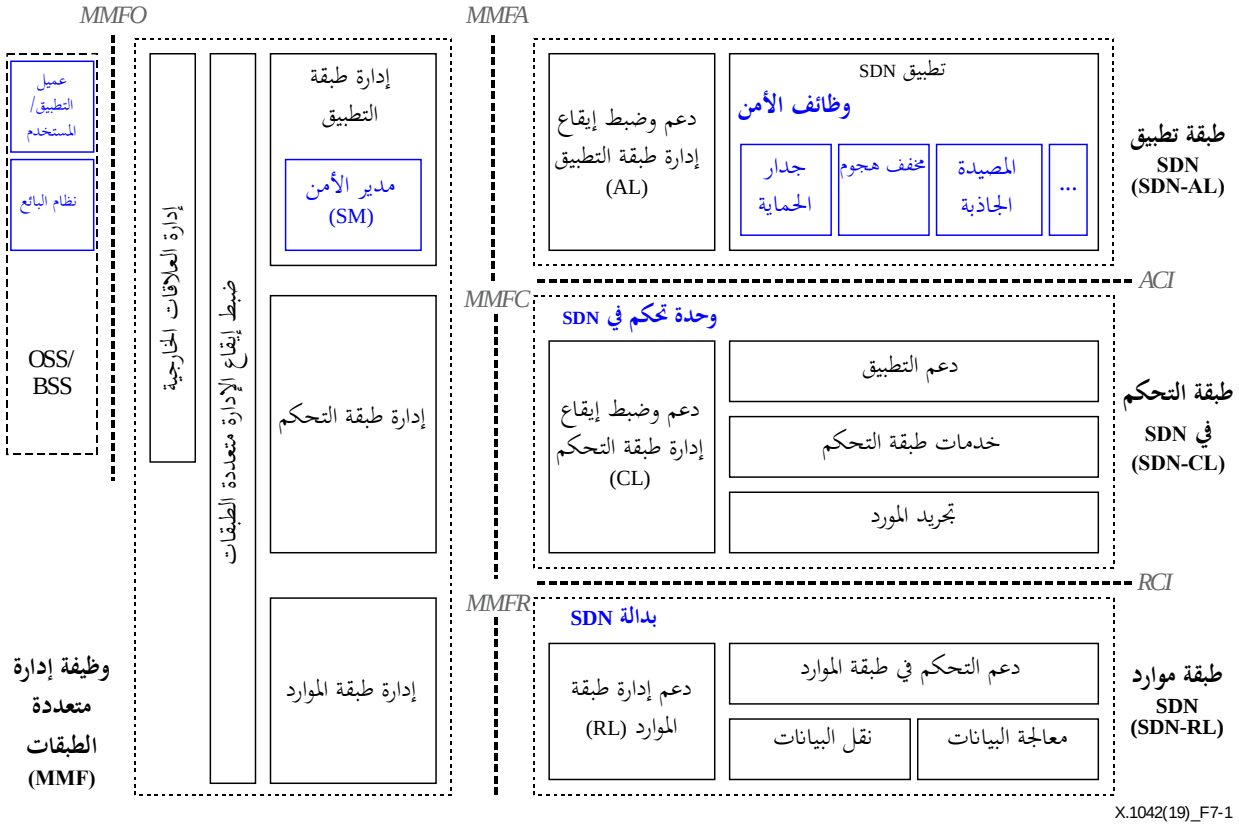
1) تطبيق التوصيل الشبكي المعرَّف بالبرمجيات (SDN): هو خدمة تبلِّغ بشكل صريح ومباشر وبرمجي متطلبات شبكتها وسلوك الشبكة المرغوب إلى وحدة تحكم في التوصيل الشبكي المعرَّف بالبرمجيات عبر سطح بيني مع المستوى الأعلى مثل طبقة التحكم في التطبيق (ACL) في الشكل 6-2. بالإضافة إلى ذلك، يمكن لتطبيقات التوصيل الشبكي المعرَّف بالبرمجيات

أن تستهلك مشهداً مجرداً للشبكة لأغراض اتخاذ القرارات الداخلية. فعلى سبيل المثال، يمكن تقديم خدمات جدار الحماية، والمصيدة الجاذبة، وتخفيف DDoS، وإدارة الأجهزة غير القانونية كتطبيقات. وتلزم تطبيقات التوصيل الشبكي المعرَّف بالبرمجيات (SDN) هذه للتفاعل مع إدارة طبقة التطبيق (ALM) من خلال دعم وضبط إيقاع إدارة طبقة التطبيق (AL-MSO) في الأعطال والتشكيلة والمحاسبة والأداء وإدارة الأمن. وعلاوة على ذلك، تضع هذه التطبيقات قواعد النفاذ، وبالتالي فهي مطلوبة أيضاً للتفاعل مع طبقة SDN-CL عبر السطوح البينية للتحكم في التطبيق (ACIs) حتى تنفَّذ قواعد النفاذ.

2) وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN): هي كيان متمركز منطقياً مسؤول عن: '1' ترجمة المتطلبات من تطبيقات التوصيل الشبكي المعرَّف بالبرمجيات إلى بدالات التوصيل الشبكي المعرَّف بالبرمجيات؛ و'2' تقديم مشاهد شبكة مجردة للتطبيقات تحتوي على معلومات مفيدة عن الشبكة مثل إحصائيات الحركة والأحداث. وبعبارة أخرى، تضع وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات قيود التدفق استناداً إلى قواعد النفاذ التي تحصل عليها من تطبيقات التوصيل الشبكي المعرَّف بالبرمجيات. لذلك، يتعين أن تتفاعل وحدة التحكم هذه مع تطبيقات CLM وSDN وطبقة SDN-RL.

3) بدالة التوصيل الشبكي المعرَّف بالبرمجيات (SDN): هي برنامج حاسوبي أو جهاز عتاد يقوم بإعادة تسيير الرزم في بيئة التوصيل الشبكي المعرَّف بالبرمجيات. وبدالات SDN قادرة على تخزين قواعد إعادة تسيير الرزمة التي تديرها وحدة تحكم SDN عبر السطح البيني مع المستوى الأدنى مثل السطح البيني للتحكم في الموارد (RCI) في الشكل 6-2. لذا، يتعين أن تتفاعل بدالة التوصيل الشبكي المعرَّف بالبرمجيات مع إدارة طبقة الموارد (RLM) وطبقة SDN-CL.

4) مدير الأمن (SM): هو وظيفة إدارة طبقة تطبيق (ALM) تنقل سياسات الأمن إلى تطبيق التوصيل الشبكي المعرَّف بالبرمجيات (SDN). لذا، يتعين على مدير الأمن التفاعل مع تطبيقات التوصيل الشبكي المعرَّف بالبرمجيات من خلال دعم وضبط إيقاع إدارة طبقة التطبيق (AL-MSO). ويوضح الشكل 7-1 موقع موارد الشبكة في الشكل 6-2. وتلزم موارد الشبكة هذه لمتابعة متطلبات [ITU Y.3301].



الشكل 7-1 – موارد الشبكة في خدمات الأمن القائمة على التوصيل الشبكي المعرَّف بالبرمجيات (SDN)

8 خدمات الأمن القائمة على التوصيل الشبكي المعرَّف بالبرمجيات (SDN)

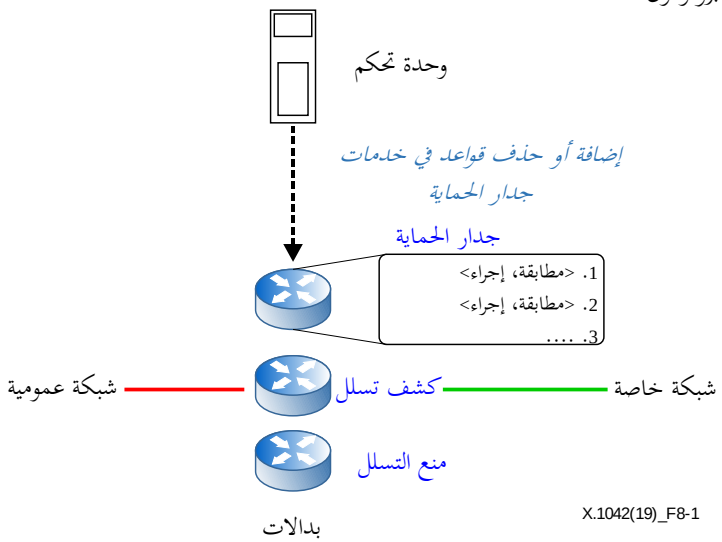
تعرِّف هذه الفقرة بخدمات الأمن باستخدام التوصيل الشبكي المعرَّف بالبرمجيات في نوعين من التوصيل الشبكي: '1' التوصيل الشبكي ضمن الميدان الواحد، مثل خدمة جدار الحماية المركزية وخدمة المصيدة الجاذبة المركزية؛ و'2' التوصيل الشبكي بين الميادين، مثل خدمة تخفيف هجمات DDoS المركزية وخدمة إدارة الأجهزة غير القانونية المركزية. والميدان في هذه التوصية يشير إلى مجموعة من موارد الشبكة التي تدار بقواعد وإجراءات مشتركة.

1.8 خدمة جدار الحماية المركزية

1.1.8 المفهوم الأساسي لخدمة جدار الحماية المركزية

تصف هذه الفقرة المفهوم الأساسي لخدمة جدار الحماية المركزية. ويمكن لهذه الخدمة إدارة موارد الشبكة بحيث يمكن إدارة قواعد جدار الحماية بمرونة. وعلى النحو المبين في الشكل 8-1، يقوم جدار الحماية المركزية بإدارة بدالات التوصيل الشبكي المعرَّف بالبرمجيات (SDN) وقواعد جدار الحماية التي يمكن إدراجها فيها أو حذفها منها.

ملاحظة – يسهل تحويل استراتيجية اصطفاء رزم صادرة عن تطبيق جدار الحماية إلى جدول تدفق عبر وحدة التحكم. ولكن بروتوكولاً بين جهاز التحكم والبدالات (مثل بروتوكولي Openflow وnetconf) لا يمكن أن يتطابق في الوقت الحالي إلا مع طبقة بروتوكول التحكم في الإرسال (TCP) ولا يوجد حقل مناظر له لتحديد معلومات تعريف رزمة البيانات فوق طبقة TCP. لذلك يتعذر تحقيق استراتيجية جدار الحماية لتحديد المعلومات فوق طبقة بروتوكول TCP دون تغيير البروتوكول.

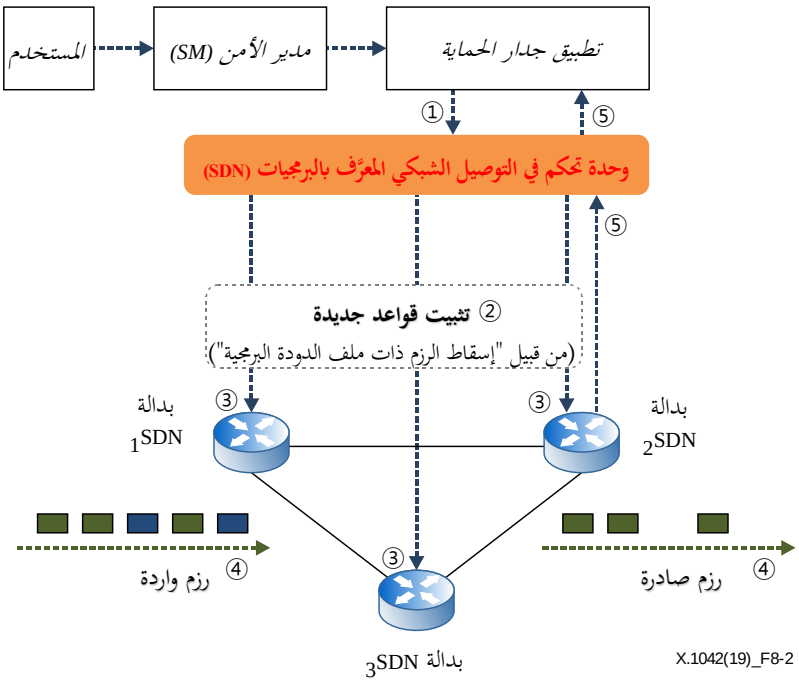


الشكل 8-1 – مفهوم خدمات جدار الحماية المركزية

2.1.8 سيناريو الخدمة في خدمة جدار الحماية المركزية

يوضح الشكل 8-2 مثالاً على سيناريو خدمة جدار الحماية المركزية لوقف انتشار دودة برمجية.

وكشرط مسبق لهذا السيناريو، ينبغي لمدير الأمن تحديد سياسة جديدة لتطبيق جدار الحماية عند التعرف على معلومات عن دودة برمجية جديدة. ولمنع انتشار الرزم بما في ذلك هذه الدودة البرمجية، يمكن للمستخدم إضافة سياسة جديدة (من قبيل "إسقاط الرزم ذات ملف الدودة البرمجية") إلى تطبيق جدار الحماية الذي يعمل على أعلى وحدة تحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN). وتمكن أيضاً إدارتها مركزياً بحيث يستطيع مدير الأمن تحديد سياسات الأمن اللازمة لتطبيق جدار الحماية عبر نقطة واحدة، أي وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات.



الشكل 8-2 – سيناريو ضمن الميدان الواحد لخدمة جدار الحماية المركزية

– الخطوة 1. يقوم تطبيق جدار الحماية بتثبيت قواعد جديدة.

وينبغي أن يضع تطبيق جدار الحماية قاعدة جديدة عند الإبلاغ عن معلومات بشأن دودة برمجية جديدة. فتضاف قاعدة جديدة (من قبيل "إسقاط الرزم ذات ملف الدودة البرمجية") إلى وحدة تحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN).

– الخطوة 2. توزع وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) قيد تدفق جديد على جميع بدالات التوصيل الشبكي المعرَّف بالبرمجيات.

ويمكن أن توزع وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات بعد تثبيتها قيد تدفق جديد على كل بدالة. ولذلك، ترسل وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات عملية إدراج تدفق تحتوي على قاعدة (من قبيل "إسقاط الرزم ذات ملف الدودة البرمجية") إلى جميع بدالات التوصيل الشبكي المعرَّف بالبرمجيات.

والدودة البرمجية الجديدة في هذه الفقرة هي إما دودة برمجية معروفة أو دودة "يوم الصِفْر". أما الدودة البرمجية المعروفة، فتُعد لها بعض الآليات مثل "التوقيعات" أو "البصمات" في خدمة جدار الحماية لكشفها والدفاع ضدها. وأما دودة "يوم الصِفْر" فينبغي تفحصها بالمسح وكشفها قبل تطبيق أي تدبير مضاد للدفاع ضدها. والديدان البرمجية تقوم بإيصال حمولات ضارة يمكنها استغلال بعض التطبيقات أو الخدمات الهشة. ويمكن اكتشاف هذه الديدان البرمجية بتفتيش حمولة رزم المستخدم. ويرد في التذييل الثاني مثال على كشف رزم البيانات بالمسح.

– الخطوة 3. تقوم جميع بدالات التوصيل الشبكي المعرَّف بالبرمجيات (SDN) بإدراج قيد التدفق الجديد في جدول التدفق الخاص بها.

وتضيف بدالة التوصيل الشبكي المعرَّف بالبرمجيات (SDN) قيد تدفق يُسقط الرزم المستقبلية الحاوية على ملفات ديدان برمجية إلى جدول التدفق عند استلام عملية قيد التدفق بشأن ملف الدودة البرمجية. وبعد ذلك، يمكن لبدالة التوصيل الشبكي المعرَّف بالبرمجيات إسقاط الرزم باستخدام ملف الدودة البرمجية.

– الخطوة 4. تنفّذ بدالة التوصيل الشبكي المعرَّف بالبرمجيات (SDN) قيود التدفق لإسقاط الرزم الحاوية ملفات الدودة البرمجية.

وتسقط بدالة التوصيل الشبكي المعرَّف بالبرمجيات (SDN) الرزم تماماً عند تلقي رزم فيها ملف الدودة البرمجية. ولا يمكن تمرير أي رزم بملف الدودة البرمجية بموجب القواعد المطبقة.

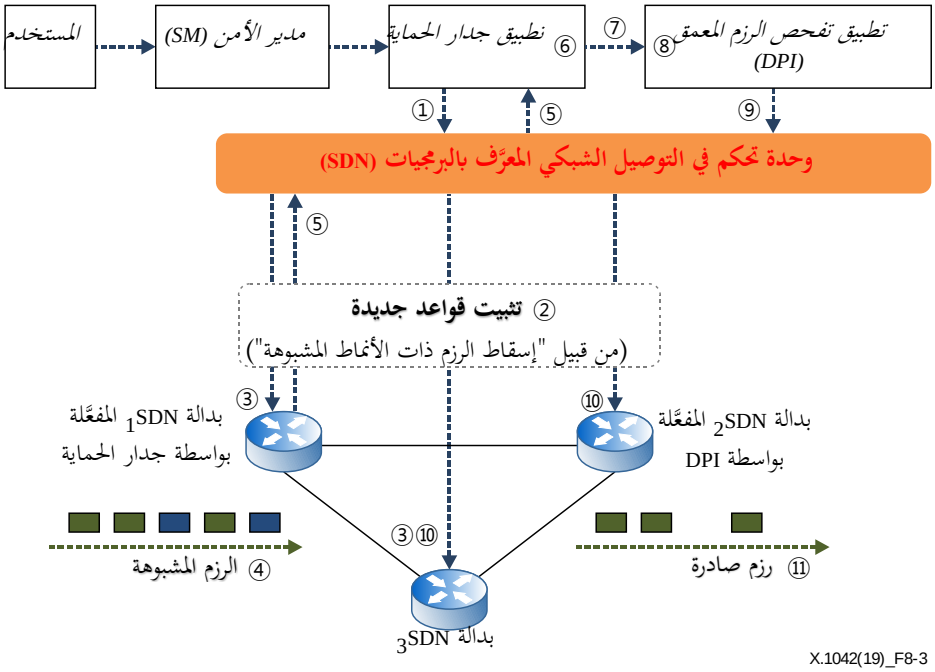
– الخطوة 5. نقوم بدالة تبديل التوصيل الشبكي المعرَّف بالبرمجيات (SDN) بإرسال تقارير إلى وحدة تحكم عند تلقي رزمة غير مألوفة.

وعندما تتلقى بدالة التوصيل الشبكي المعرَّف بالبرمجيات (SDN) نوعاً من الرزم لم يعالَج من قبل، فإنها تحذف هذه الرزمة وترسل تقريراً إلى وحدة التحكم عن هذا النوع من الرزم. وتحلل وحدة التحكم ما إذا كان ذلك هجوماً. فإذا كان هجوماً، تقوم وحدة التحكم بإرسال رسالة إلى تطبيق جدار الحماية وتنفَّذ الخطوة 1. وإذا لم يكن كذلك، تحتفظ وحدة التحكم بقيد تدفق منتظم للإيعاز للبدالات بكيفية التعامل مع هذا التسلسل في الرزم اللاحقة.

3.1.8 سيناريو الخدمة في خدمة جدار الحماية التعاونية

يوضح الشكل 3-8 مثالاً على سيناريو تطبيق جدار الحماية التعاونية مع تطبيق تفحص الرزم المعمق (DPI) لتحقيق مراقبة وإدارة مركزية لتدفق لبروتوكول الاتصالات الصوتية عبر بروتوكول الإنترنت (VoIP)/بروتوكول الاتصالات الصوتية عبر التطور الطويل الأجل (VoLTE). ويوضح هذا السيناريو أن تطبيق DPI يتحكم في كل بدالة توصيل شبكي معرَّف بالبرمجيات (SDN) لإدارة تدفق مكالمات VoIP/VoLTE من خلال معالجة القواعد الممكن إضافتها أو حذفها أو تعديلها دينامياً. ويمكن لهذا التطبيق التعاون مع تطبيق جدار الحماية لحماية خدمة VoIP/VoLTE. وعلى وجه التحديد، تجري بدالة مفعَّلة بجدار الحماية تحققات أمنية أساسية من رزم التدفقات المجهولة. وإذا اكتشفت البدالة أن الرزمة هي رزمة تدفق مكالمات VoIP مجهولة تُظهر بعض الأنماط المشبوهة، فإنها تُقلع وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات كي قوم بتحليل أمني أكثر تخصصاً لرزمة مكالمة VoIP المشبوهة.

وكشرط مسبق لهذا السيناريو، ينبغي لمدير الأمن وضع سياسة جديدة لجدار الحماية وتطبيق DPI عند التعرف على معلومات عن نمط مشبوه. ولمنع الرزم من تضمين هذه الأنماط، يضيف المستخدم السياسة الجديدة (من قبيل "إسقاط الرزم ذات الأنماط المشبوهة") إلى جدار الحماية وتطبيق DPI العاملان فوق وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN). ويمكن أيضاً إدارتها مركزياً بحيث يمكن أن يضع مدير الأمن سياسات الأمن للتطبيقات عبر نقطة واحدة، أي وحدة تحكم في التوصيل الشبكي المعرَّف بالبرمجيات.



الشكل 3-8 – سيناريو ضمن الميدان الواحد لخدمة جدار الحماية التعاونية

– الخطوة 1. يقوم تطبيقا جدار الحماية وتفحص الرزم المعمق (DPI) بتثبيت قواعد جديدة للنمط المعروف.

وينبغي أن تحدد تطبيقات جدار الحماية وDPI قاعدة جديدة عند الإبلاغ عن المعلومات بشأن نمط جديد. وتضاف قاعدة جديدة (من قبيل إيصال الرزم ذات النمط إلى وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN)) إلى وحدة تحكم في التوصيل الشبكي المعرَّف بالبرمجيات.

– الخطوة 2. توزع وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) قيد تدفق جديد على جميع بدالات التوصيل الشبكي المعرَّف بالبرمجيات.

ويمكن أن توزع وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات قيد تدفق جديد على كل بدالة. ولذلك، ترسل وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) عملية إدراج تدفق تحتوي على قاعدة (من قبيل إيصال الرزم ذات النمط) إلى جميع بدالات التوصيل الشبكي المعرَّف بالبرمجيات. وإذا كان لكل بدالة وظيفة مختلفة، ترسل وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات قيود تدفق مختلفة في كل عملية. أي ينبغي ألا تحصل البدالات المفعَّلة بجدار الحماية على قيود التدفق المتعلقة بتفحص الرزم المعمق (DPI).

– الخطوة 3. تقوم جميع بدالات التوصيل الشبكي المعرَّف بالبرمجيات (SDN) بإدراج قيد التدفق الجديد في جداول التدفق الخاص بها.

وتضيف بدالة التوصيل الشبكي المعرَّف بالبرمجيات (SDN) قيد تدفق من أجل إيصال رزم مستقبلية ذات النمط المشبوه في جدول تدفقها عند استقبال عملية قيد التدفق من وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات.

– الخطوة 4. تنفّذ بدالة التوصيل الشبكي المعرَّف بالبرمجيات (SDN) قيود التدفق لإيصال الرزم الحاوية ملفات مشبوهة.

وتقوم بدالة التوصيل الشبكي المعرَّف بالبرمجيات (SDN) بإيصال الرزم عند استقبال رزم ذات نمط مشبوه في وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات. وينبغي نقل الرزم ذات الأنماط المشبوهة كافة إلى وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) بموجب القواعد المطبقة.

– الخطوة 5. تقوم بدالة التوصيل الشبكي المعرَّف بالبرمجيات (SDN) ووحدة التحكم بإعادة التسيير نحو تطبيق جدار الحماية عند تلقي رزمة غير مألوفة.

وعندما تتلقى وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) نوعاً من الرزم لم تعالجه من قبل، تقوم بإعادة تسيير هذه الرزم إلى تطبيق جدار الحماية كي تخضع لتفتيش أمني أساسي.

– الخطوة 6. يقوم تطبيق جدار الحماية بتحليل الرزمة غير المألوفة.

ويقوم تطبيق جدار الحماية بتحليل حقول رأسية الرزمة ويقرر أنها رزمة مجهولة لإشارة تدفق مكالمات VoIP من قبيل رزمة بروتوكول استهلال الدورة (SIP) ذات نمط مشبوه.

– الخطوة 7. يقوم تطبيق جدار الحماية بإطلاق تطبيق تفحص الرزم المعمق (DPI).

ويقوم تطبيق جدار الحماية بتشغيل تطبيق مناسب مثل تطبيق DPI للتحليل الأمني التفصيلي لرزم الإشارات المشبوهة. وبعد ذلك، يقوم بإعادة تسيير الرزم إلى تطبيق DPI.

– الخطوة 8. يحلل تطبيق DPI الرزمة غير المألوفة.

ويحلل تطبيق DPI رأسيات ومحتويات رزمة الإشارة مثل رقم الاتصال ورأسيات وصف الدورة. فعلى سبيل المثال، إذا اعتبر تطبيق DPI الرزمة رزمةً مخادعة من قبل متسللين أو رزمة مسح تبحث عن أجهزة VoIP/VoLTE، فإنه يسقط الرزمة.

– الخطوة 9: يطلب تطبيق DPI من وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) حظر هذه الرزمة.

يطلب تطبيق DPI من وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) حظر تلك الرزمة والرزم اللاحقة ذات معرف المكالمة نفسه.

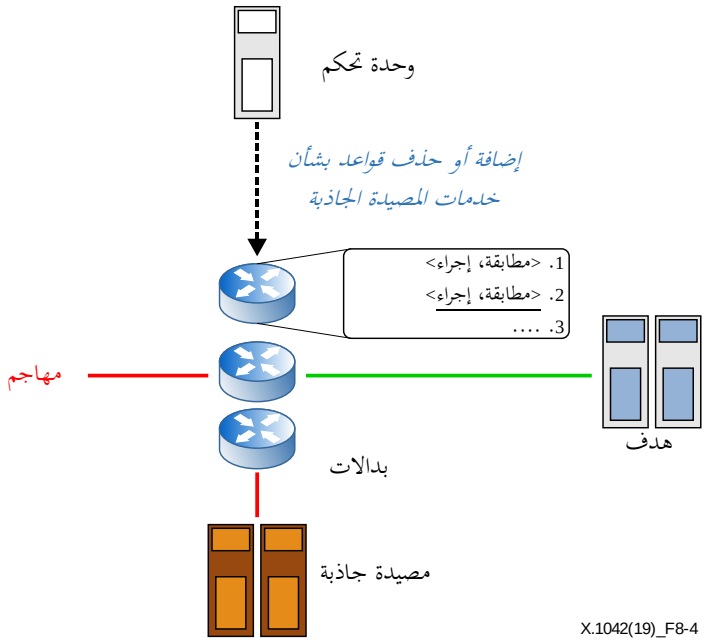
– الخطوة 10. تقوم وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) بتثبيت قواعد جديدة.

وتوزع وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) قيد تدفق جديد (من قبيل "إسقاط الرزم") إلى بدالات التوصيل الشبكي المعرَّف بالبرمجيات كافة كما في الخطوة 2. وبعد ذلك، ستقوم هذه البدالات بإسقاط الرزم غير القانونية كافة.

2.8 خدمة المصيدة الجاذبة المركزية

1.2.8 المفهوم الأساسي لخدمة المصيدة الجاذبة المركزية

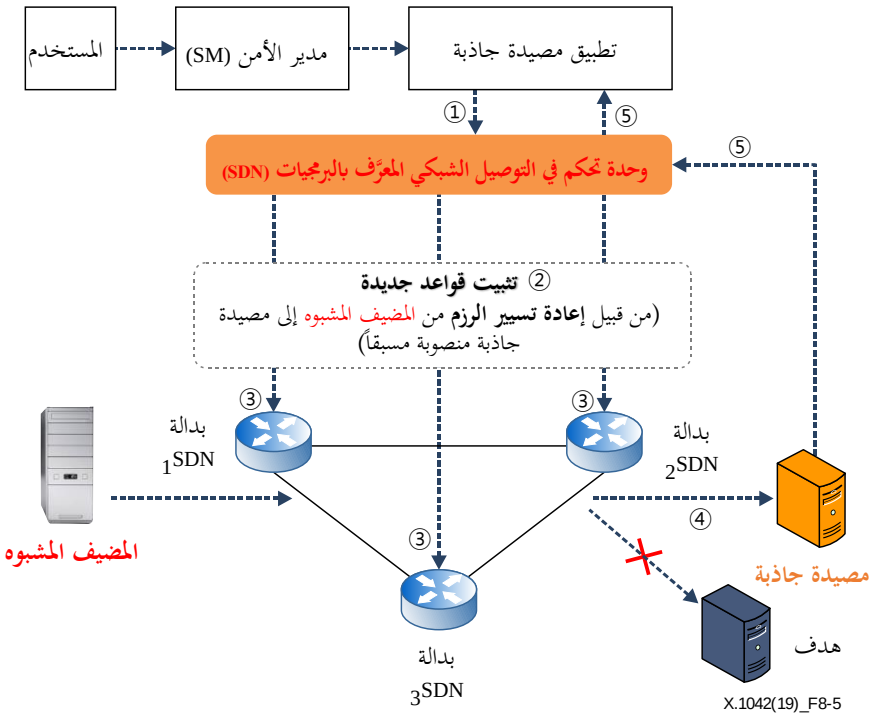
تصف هذه الفقرة المفهوم الأساسي لخدمة المصيدة الجاذبة المركزية. ويمكن للمصيدة الجاذبة إدارة أماكنها دينامياً. وعلى النحو المبين في الشكل 8-4، تدير مصيدة جاذبة مركزية بدالات ومسارات التسيير الجديدة لجذب المهاجمين إلى مكان يستخدم كفخ، أي كمصيدة جاذبة. وتشكَّل المصيدة الجاذبة كهدف للهجوم المزمع ويبلغ المعلومات التي تُجمع إلى خدمة المصيدة الجاذبة المركزية.



الشكل 8-4 – مفهوم خدمة المصيدة الجاذبة المركزية

2.2.8 سيناريو الخدمة للمصيدة الجاذبة المركزية

يوضح الشكل 8-5 مثالاً على سيناريو خدمة مصيدة جاذبة لإضافة مسار تسيير إلى مصيدة جاذبة بدلاً من الهدف الفعلي المتمثل في بدالات التوصيل الشبكي المعرَّف بالبرمجيات (SDN).



الشكل 8-5 – سيناريو ضمن الميدان الواحد لخدمة مصيدة جاذبة مركزية

– الخطوة 1. يقوم تطبيق مصيدة جاذبة بتثبيت قواعد جديدة على وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات.

وينبغي أن يحدد تطبيق مصيدة جاذبة قاعدة جديدة عند الإبلاغ عن معلومات بشأن مضيف ما مشبوه. ومن أجل مراقبة الحركة من المضيف المشبوه، تضاف القاعدة الجديدة (من قبيل "إعادة تسيير الرزم من المضيف المشبوه إلى مصيدة جاذبة") إلى وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) بواسطة تطبيق مصيدة جاذبة قيد التشغيل فوق وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات.

– الخطوة 2. توزع وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) قواعد جديدة على بدالات التوصيل الشبكي المعرَّف بالبرمجيات المناسبة.

ويمكن أن توزع وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات بعد تثبيتها قاعدة جديدة على كل بدالة. ولذلك، ترسل وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات عملية إدراج تدفق تحتوي على قاعدة (من قبيل "إعادة تسيير الرزم من المضيف المشبوه إلى مصيدة جاذبة") إلى جميع بدالات التوصيل الشبكي المعرَّف بالبرمجيات. ويمكن أيضاً إدارتها مركزياً بحيث يستطيع مدير الأمن تحديد سياسات الأمن لخدمتها عبر نقطة واحدة، أي وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات.

– الخطوة 3. تقوم جميع بدالات التوصيل الشبكي المعرَّف بالبرمجيات (SDN) بإدراج قواعد جديدة في جداول التدفق الخاصة بها.

وتضيف كل بدالات التوصيل الشبكي المعرَّف بالبرمجيات (SDN) إلى جداول التدفق لديها قيد تدفق إعادة تسيير رزم مستقبلية من المضيف المشبوه إلى مصيدة جاذبة عند تلقي عملية إدراج التدفق بشأن المضيف المشبوه. وبعد ذلك، يمكن لبدالة التوصيل الشبكي المعرَّف بالبرمجيات إعادة تسيير الرزم من المضيف المشبوه إلى مصيدة جاذبة.

– الخطوة 4. تقوم بدالة التوصيل الشبكي المعرَّف بالبرمجيات (SDN) بتنفيذ قواعد جديدة لدعم خدمة المصيدة الجاذبة.

ويمكن لبدالة التوصيل الشبكي المعرَّف بالبرمجيات (SDN) إعادة تسيير الرزم إلى مصيدة جاذبة عندما تتلقى الرزم من المضيف المشبوه. ولا يمكن تمرير أي رزم من المضيف المشبوه إلى بدالة مضيف هدف فعلي في إطار القواعد المطبقة. وتُجمع الرزم المعاد تسييرها في المصيدة الجاذبة.

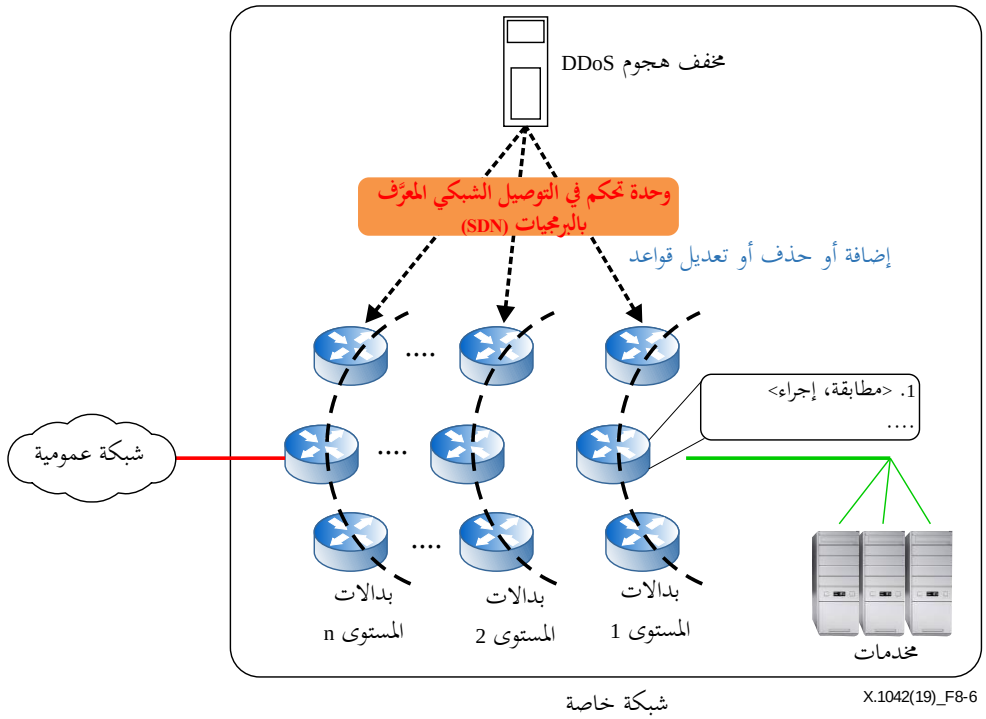
– الخطوة 5. تقدم خدمة مصيدة جاذبة تقريراً إلى وحدة التحكم عن الرزم المشبوهة.

وعندما تتلقى خدمة مصيدة جاذبة رزم من مضيفات مشبوهة، فإنها تعالج هذه الرزم وترسل تقريراً إلى وحدة التحكم عن هذا النوع من الرزم لدعم تحليل رزم وحدة التحكم.

3.8 خدمة تخفيف هجوم الحرمان من الخدمة الموزَّع (DDoS) المركزية

1.3.8 المفهوم الأساسي لخدمة تخفيف هجوم الحرمان من الخدمة الموزَّع (DDoS) المركزية

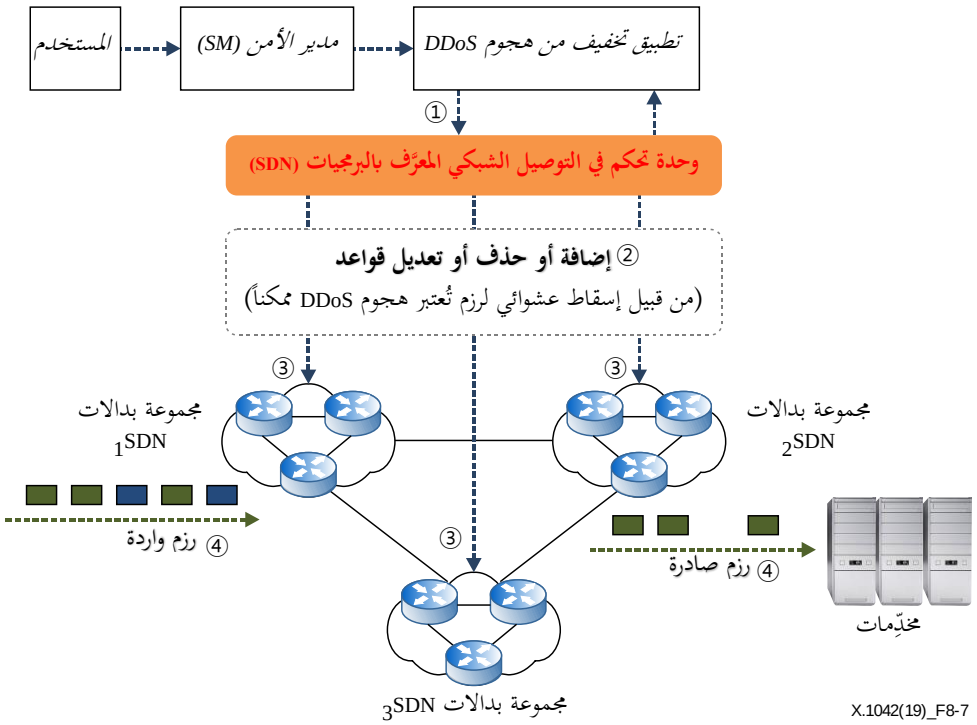
يوضح الشكل 6-8 خدمة مركزية لتخفيف هجوم الحرمان من الخدمة الموزَّع (DDoS) تقوم هذه الخدمة بالإضافة إلى القواعد أو الحذف منها أو تعديلها في كل بدالة توصيل شبكي معرَّف بالبرمجيات (SDN). بخلاف "خدمة جدار الحماية المركزية" المرتبطة بما يقع ضمن الميدان الواحد، تركز هذه الخدمة بشكل أساسي على الميدان البيني.



الشكل 6-8 – مفهوم خدمات تخفيف هجوم DDoS المركزية

2.3.8 خدمة تخفيف هجوم DDoS المركزية بالمخدِّمات الخالية من حالة مخزَّنة

يوضح الشكل 7-8 مثال سيناريو لخدمة تخفيف مركزي من هجوم DDoS بمخدِّمات خدمة اسم الميدان (DNS) الخالية من حالة مخزَّنة.



الشكل 8-7 سيناريو بين الميادين لخدمة تخفيف مركزي من هجوم DDoS بمخدِّمات خالية من حالة مخزَّنة

– الخطوة 1. يقوم تطبيق التخفيف بتثبيت قواعد جديدة لوحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات وينبغي أن يحدد تطبيق تخفيف هجوم DDoS قاعدة جديدة عند العلم بهجوم DDoS جديد من مدير الأمن. ولمنع وصول الرزم إلى المخدِّمات وإهدار موارد المخدِّمات، تضاف إلى وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات قاعدة جديدة (من قبيل "إسقاط عشوائي لرزم هجوم DDoS باحتمال معين"). وتنفَّذ إضافة القاعدة بواسطة تطبيق تخفيف هجوم DDoS المشغَّل فوق وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات.

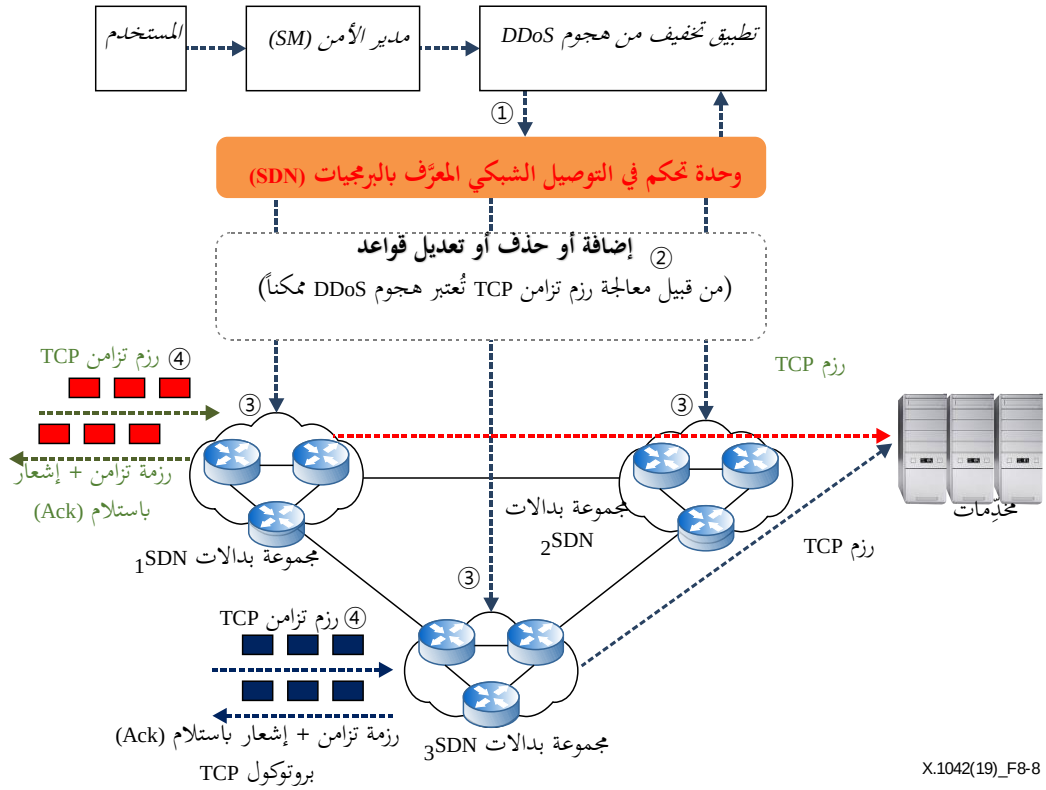
– الخطوة 2. تقوم وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) بتوزيع قواعد جديدة على البدالات المناسبة. ويمكن أن توزع وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات بعد تثبيتها قاعدة جديدة على كل بدالة. ولذلك، ترسل وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات عملية إدراج تدفق تحتوي على قاعدة (من قبيل "إسقاط عشوائي لرزم تُعتبر هجوم DDoS ممكناً احتمال معين") إلى جميع بدالات التوصيل الشبكي المعرَّف بالبرمجيات. ويمكن أيضاً إدارتها مركزياً بحيث يستطيع مدير الأمن تحديد سياسات الأمن لخدمتها عبر نقطة واحدة، أي وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات.

– الخطوة 3: تقوم جميع بدالات التوصيل الشبكي المعرَّف بالبرمجيات (SDN) بإدراج قواعد جديدة في جداول التدفق الخاصة بها. وتضيف كل بدالات التوصيل الشبكي المعرَّف بالبرمجيات إلى جداول تدفقها قيد تدفق يسقط الرزم المستقبلية التي تُعتبر رزم هجمات DDoS عند استلام عملية إدراج تدفق بشأن تخفيف هجوم DDoS. وبعد ذلك، يمكن لبدالة التوصيل الشبكي المعرَّف بالبرمجيات (SDN) بين بدالات في الميدان إسقاط رزم هجوم DDoS باحتمال يتناسب مع شدة هجوم DDoS.

– الخطوة 4. تقوم بدالة التوصيل الشبكي المعرَّف بالبرمجيات بتنفيذ قواعد جديدة للتخفيف من هجوم DDoS. وتسقط بدالة التوصيل الشبكي المعرَّف بالبرمجيات (SDN) الرزم تماماً بشكل انتقائي عند تلقي رزم هجوم DDoS. وتُسقَط رزم هجمات DDoS عشوائياً من خلال بدالات التوصيل الشبكي المعرَّف بالبرمجيات (SDN) في كل ميدان وفقاً لإمكانيات المعالجة وميزات الميادين. بعد ذلك، ينبغي إبلاغ وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات عن نتائج الإسقاطات.

3.3.8 خدمة تخفيف هجوم DDoS المركزية بالمخدِّمات ذات الحالة المخزَّنة

يوضح الشكل 8-8 مثال سيناريو لتخفيف مركزي من هجوم DDoS بمخدِّمات على شبكة الإنترنت ذات حالة مخزَّنة



الشكل 8-8 – سيناريو بين الميادين لتخفيف مركزي من هجوم DDoS بمخدِّمات ذات حالة مخزَّنة

– الخطوة 1. يقوم تطبيق التخفيف بتثبيت قواعد جديدة لوحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات وينبغي أن يختار تطبيق تخفيف هجوم DDoS البدالة التي تقوم بدور وكيل خدمة TCP. وتنفَّذ إضافة قاعدة جديدة بواسطة تطبيق تخفيف هجوم DDoS المشغَّل فوق وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات.

– الخطوة 2. تقوم وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات بتوزيع قواعد جديدة على البدالات المناسبة.

ويمكن أن توزع وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات بعد تثبيتها قاعدة جديدة على بدالات تخفيف هجوم DDoS المناسبة. ولذلك، ترسل وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات عملية إدراج تدفق تحتوي على قاعدة (من قبيل "توليد رزم تزامن – إشعار باستلام بروتوكول TCP (TCP Sync-Ack) لرزم تُعتبر هجمات DDoS") إلى جميع بدالات التوصيل الشبكي المعرَّف بالبرمجيات. لذلك، تثبَّت قاعدة جديدة في البدالة المختارة بحيث يمكنها توليد رزم TCP Sync-Ack لتزامن TCP كطلبات. وفي حال وصول نفس الطلبات بمعدل تكرار أكبر من المعدل المتوقع، تختار وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) بدالة تبديل جديدة بحيث تقوم البدالة بدور المخدِّم. وفي تزامن TCP العادي، تنقل البدالة دورة TCP إلى المخدِّم المقابل في الشبكة الخاصة. ويمكن أيضاً إدارتها مركزياً بحيث يستطيع مدير الأمن تحديد سياسات الأمن لخدمتها عبر نقطة واحدة، أي وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات.

– الخطوة 3. تنطبق جميع بدالات التوصيل الشبكي المعرَّف بالبرمجيات (SDN) على القواعد الجديدة في جدول التدفق الخاص بها.

وتضيف كل بدالات التوصيل الشبكي المعرَّف بالبرمجيات إلى جداول تدفقها قيد تدفق يسقط الرزم المستقبلية التي تُعتبر رزم هجمات DDoS عند استلام عملية إدراج تدفق بشأن تخفيف هجوم DDoS. وبعد ذلك، يمكن لبدالة التوصيل الشبكي المعرَّف بالبرمجيات (SDN) توليد رزم TCP Sync-Ack باحتمال يتناسب مع شدة هجوم DDoS.

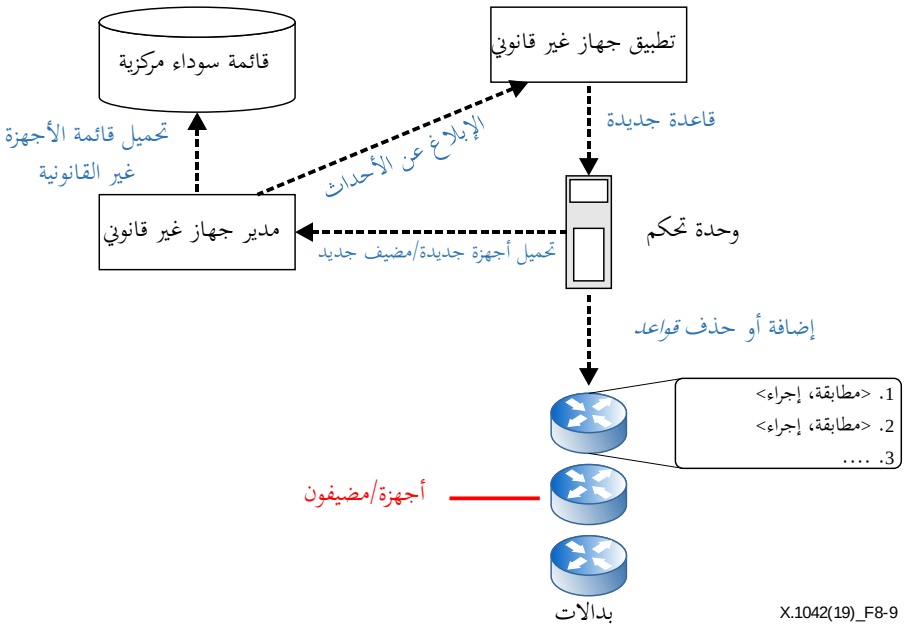
– الخطوة 4. تقوم بدالة التوصيل الشبكي المعرَّف بالبرمجيات بتنفيذ قواعد جديدة للتخفيف من هجوم DDoS.

وتستجيب بدالة التوصيل الشبكي المعرَّف بالبرمجيات (SDN) تماماً وعشوائياً لرزم TCP Sync من مضيف خصم عند تلقي رزم هجوم DDoS. ويُتعامل مع طلبات هجمات DDoS للمخدِّمات ذات الحالة المخزنة بواسطة بدالات بدلاً من المخدِّمات الفعلية. وتُسقَط رزم هجمات DDoS عشوائياً من خلال بدالات التوصيل الشبكي المعرَّف بالبرمجيات (SDN) في كل ميدان وفقاً لإمكانيات المعالجة وميزات الميادين. بعد ذلك، ينبغي إرسال نتيجة تنفيذ بدالة التوصيل الشبكي المعرَّف بالبرمجيات للتخفيف من هجوم DDoS إلى وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات.

4.8 الخدمة المركزية لإدارة الأجهزة غير القانونية

1.4.8 المفهوم الأساسي للخدمة المركزية لإدارة الأجهزة غير القانونية

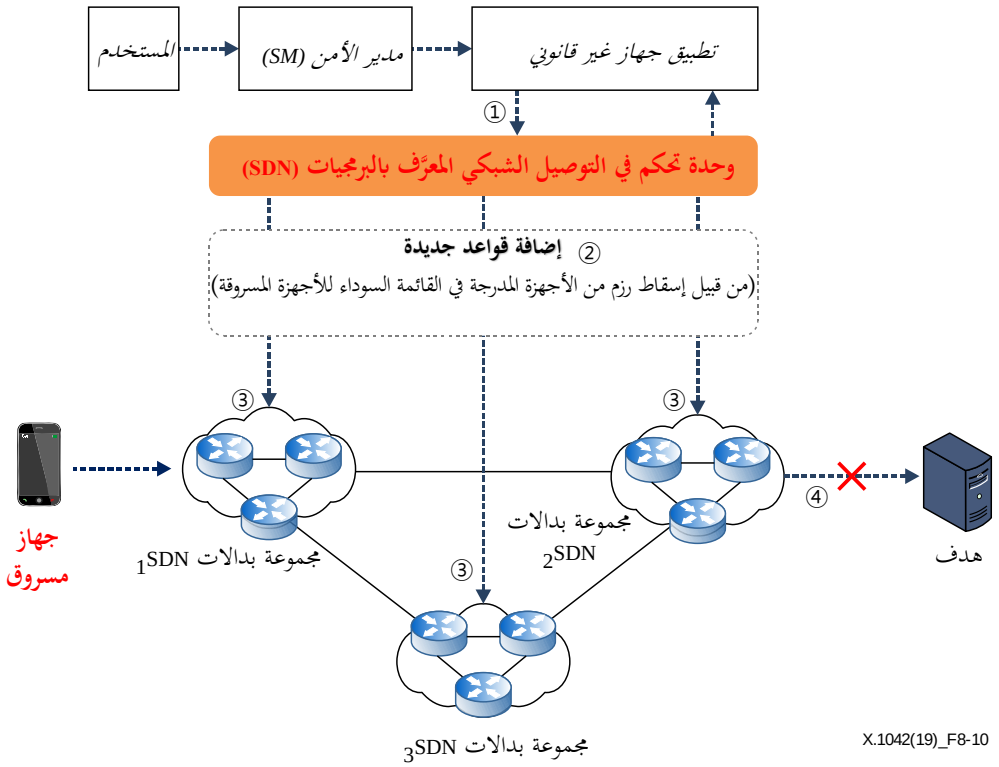
تصف هذه الفقرة المفهوم الأساسي للخدمة المركزية لإدارة الأجهزة غير القانونية. وعلى النحو المبين في الشكل 8-9، تدير الخدمة المركزية لإدارة الأجهزة غير القانونية القائمة السوداء للأجهزة غير القانونية لمنع الحركة من تلك الأجهزة. وتخزَّن قائمة الأجهزة غير القانونية في قاعدة بيانات القائمة السوداء ويمكن تحديثها إما يدوياً أو تلقائياً بواسطة تطبيقات مستقلة. ويحمّل المدير المركزي للأجهزة غير القانونية قائمة الأجهزة غير القانونية من قاعدة بيانات القائمة السوداء ويقدم تقريراً عن تلك الأحداث إلى تطبيق الأجهزة غير القانونية الذي ينشئ قواعد أمنية جديدة لمنع حركة الشبكة من/إلى تلك الأجهزة غير القانونية.



الشكل 8-9 – مفهوم الخدمة المركزية لإدارة الأجهزة غير القانونية

2.4.8 سيناريو الخدمة في خدمة مركزية لإدارة الأجهزة غير القانونية

يعرض الشكل 8-10 مثالاً على سيناريو خدمة مركزية لإدارة الأجهزة غير القانونية بغية منع الحركة من جهاز متنقل مسروق.



الشكل 8-10 – سيناريو الميدان البيني في الخدمة المركزية لإدارة الأجهزة غير القانونية

– الخطوة 1. يقوم تطبيق إدارة الجهاز غير القانوني بتثبيت قواعد جديدة.

وينبغي أن يحدد تطبيق جهاز غير قانوني قاعدة جديدة عند إبلاغ المدير المركزي للجهاز غير القانوني عن معلومات بشأن أجهزة مسروقة جديدة. وكشرط مسبق لهذا السيناريو، يضيف تطبيق الجهاز غير القانوني أو مدير الأمن (SM) قاعدة جديدة (من قبيل "إسقاط رزم من الأجهزة المخزنة في قائمة سوداء مركزية للأجهزة المسروقة") إلى وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN).

– الخطوة 2. تقوم وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات بتوزيع قواعد جديدة.

ويمكن أن توزع وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات بعد تثبيتها قاعدة جديدة. ولذلك، ترسل وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات عملية إدراج تدفق تحتوي على قاعدة (من قبيل "إسقاط رزم من الأجهزة المسروقة الجديدة") إلى جميع بدالات التوصيل الشبكي المعرَّف بالبرمجيات. ويمكن أيضاً إدارتها مركزياً بحيث يستطيع مدير مركزي للجهاز غير القانوني أو مدير الأمن تحديد سياسات الأمن لخدمتها عبر نقطة واحدة، أي وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات.

– الخطوة 3. تقوم جميع بدالات التوصيل الشبكي المعرَّف بالبرمجيات (SDN) بإدراج قواعد جديدة في جداول التدفق الخاصة بها.

وتضيف كل بدالات التوصيل الشبكي المعرَّف بالبرمجيات إلى جداول تدفقها قيد تدفق يسقط الرزم المستقبلية من تلك الأجهزة عند استلام عملية إدراج تدفق بشأن الأجهزة المسروقة.

– الخطوة 4. تقوم بدالة التوصيل الشبكي المعرَّف بالبرمجيات بتنفيذ قواعد جديدة للتخفيف من هجوم DDoS.

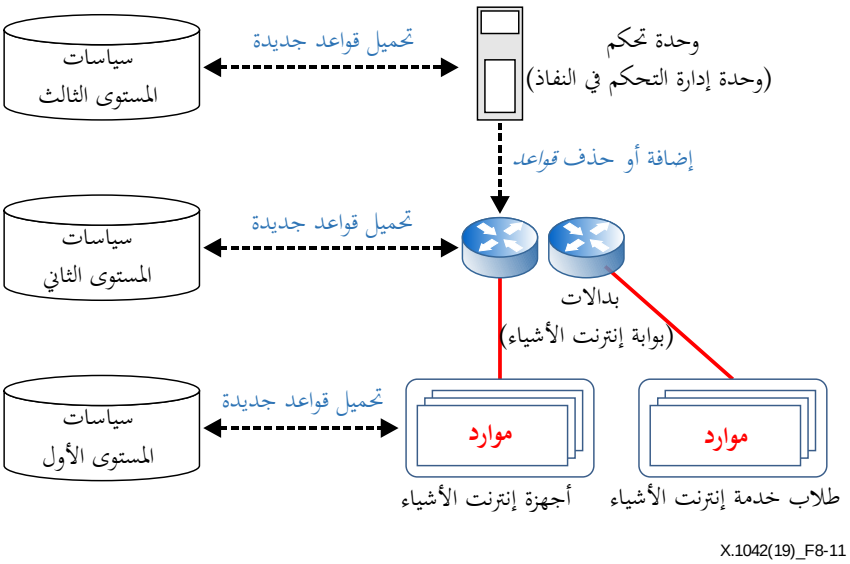
وتسقط بدالة التوصيل الشبكي المعرَّف بالبرمجيات (SDN) الرزم تماماً عند تلقي رزم من تلك الأجهزة. ولا يمكن تمرير أي رزم من هذه الأجهزة ضمن القواعد المطبقة. وبعد ذلك، ينبغي إرسال نتيجة التنفيذ إلى وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات.

ملاحظة – من المهم التعرف على الأجهزة غير القانونية. وتُستخدم هوية فريدة يخصصها المدير المركزي لتحديد هوية جهاز غير قانوني. وإذا اكتفت وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) بالتعرف على عنوان شبكة يمكن تغييره دينامياً مثل عنوان IP وعنوان MAC لجهاز، تثبَّت قاعدة جديدة وتُحذف القاعدة القديمة على وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات في كل مرة يتغير فيها عنوان الشبكة لجهاز غير قانوني.

5.8 خدمة إدارة التحكم في النفاذ

1.5.8 المفهوم الأساسي لخدمة إدارة التحكم في النفاذ

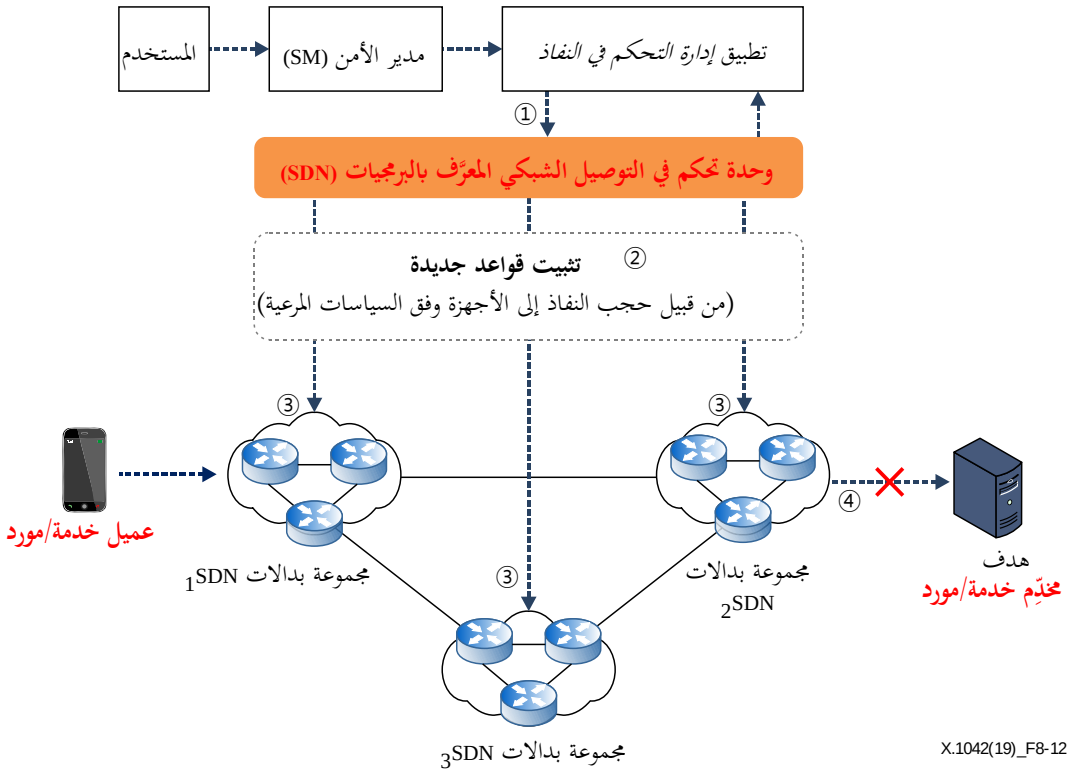
تصف هذه الفقرة المفهوم الأساسي لخدمة إدارة التحكم في النفاذ (ACM). يمكن لوحدة إدارة التحكم في النفاذ ذات وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) أن تدير سياسات حقوق النفاذ تراتبياً. وعلى النحو المبين في الشكل 8-11، تقوم وحدة ACM بإدارة حقوق النفاذ لمنع النفاذ غير القانوني إلى الموارد.



الشكل 8-11 – مفهوم خدمة إدارة التحكم في النفاذ

2.5.8 سيناريو الخدمة في خدمة إدارة التحكم في النفاذ

يوضح الشكل 8-12 مثالاً على سيناريو خدمة إدارة التحكم في النفاذ (ACM) التي تديرها وحدة تحكم في الأمن. يتضمن هذا السيناريو وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) وبدالات.



الشكل 8-12 – سيناريو الميدان البيني لخدمة إدارة التحكم في النفاذ

– الخطوة 1. يقوم تطبيق إدارة التحكم في النفاذ بتثبيت سياسات جديدة واردة من مدير الأمن.

وينبغي أن يحدد تطبيق إدارة التحكم في النفاذ (ACM) سياسات جديدة للنفاذ إلى الموارد في أجهزة الخدمة/الموارد الموزعة (مثل أجهزة إنترنت الأشياء). وكشرط مسبق لهذا السيناريو، يضيف مدير الأمن سياسات جديدة بالفعل إلى تطبيق ACM هذا.

– الخطوة 2. تقوم وحدة تحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN) بتوزيع قواعد جديدة.

ينبغي تخزين قاعدة أو قواعد جديدة. وبعد ذلك، يمكن توزيعها على كل بدالة من خلال وحدة تحكم في التوصيل الشبكي المعرَّف بالبرمجيات (SDN). ويجوز أن ترسل وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات طلب نفاذ لتشغيل المورد (الموارد) في جهاز خدمة/مورد. وفي هذه الحالة، لا تتلقى وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات أي طلبات من بدالات التوصيل الشبكي المعرَّف بالبرمجيات لتوزيع القواعد. وقد تتمكن بدالات التوصيل الشبكي المعرَّف بالبرمجيات من مطالبة وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات بمنح قواعد النفاذ للموارد في أجهزة الخدمة/الموارد قبل إرسال طلبات توزيع القواعد إلى وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات.

– الخطوة 3. تضيف كل بدالات التوصيل الشبكي المعرَّف بالبرمجيات (SDN) قواعد جديدة إلى قاعدة البيانات المحلية الخاصة بها.

وتضيف جميع بدالات التوصيل الشبكي المعرَّف بالبرمجيات قواعد جديدة إلى قواعد البيانات المحلية الخاصة بها لمعالجة طلبات إجازة النفاذ إلى أجهزة الخدمة/الموارد.

– الخطوة 4. تقوم بدالة التوصيل الشبكي المعرَّف بالبرمجيات (SDN) بتنفيذ القواعد الجديدة.

ويمكن لبدالة التوصيل الشبكي المعرَّف بالبرمجيات (SDN) إسقاط الرزم بالكامل عند تلقي الرزم من عميل خدمة/مورد وفقاً لقواعد النفاذ. وهنا، ينبغي أن يكون لكل ميدان بدالة توصيل شبكي معرَّف بالبرمجيات قواعد بيانات مختلفة وفقاً لإمكانيات كل ميدان. ولا يمكن تمرير أي رزم من هؤلاء العملاء عبر بدالة التوصيل الشبكي المعرَّف بالبرمجيات بموجب القواعد المطبقة. وينبغي الإبلاغ عن أي رزمة لا تحتوي على أي قواعد نفاذ إلى وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات من أجل إدارتها من خلال تطبيق ACM.

التذييل I

معايير لخدمات الأمن القائمة على التوصيل الشبكي المعرَّف بالبرمجيات (SDN)

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يقدم هذا التذييل معايير لمختلف خدمات الأمن.

1.I معايير لخدمات الأمن في الشبكات ضمن الميدان الواحد

1.1.I خدمة جدار الحماية المركزية

تواجه جدران الحماية التقليدية تحديات في مجالات مثل التكاليف الكبيرة والأداء وإدارة التحكم في النفاذ ووضع سياسة مرعية وآليات نفاذ قائمة على الرزم. وللتعامل مع هذه التحديات، تعرض هذه التوصية إطار خدمة جدار حماية مركزية قائمة على التوصيل الشبكي المعرَّف بالبرمجيات (SDN). ويمكن إدارة قواعد جدار الحماية بمرونة بواسطة مخدِّم مركزي. ويمكن استخدام بروتوكولات التوصيل الشبكي المعرَّف بالبرمجيات القائمة من خلال سطوح بينية معيارية بين تطبيقات وبدالات جدار الحماية.

- التكلفة

تعتبر تكلفة إضافة جدران الحماية إلى موارد الشبكة مثل المسيِّرات والبوابات والبدالات تكلفة كبيرة لأن الحاجة تدعو لإضافة جدران حماية إلى كل مورد شبكي. وللتغلب على هذا الإشكال، يمكن إدارة كل مورد شبكي مركزياً بحيث يتعامل مخدِّم مركزي مع جدار حماية واحد.

- الأداء

كثيراً ما يكون أداء جدران الحماية أبطأ من سرعة وصلة السطوح البينية لشبكتها. ويحتاج كل مورد شبكي للتحقق من قواعد جدار الحماية دون الرجوع إلى ظروف الشبكة. ويمكن نشر جدران الحماية بشكل متكيف وفقاً لظروف الشبكة في هذا الإطار.

- إدارة التحكم في النفاذ

نظراً لوجود مئات من موارد الشبكة في شبكة مدارة، فإن الإدارة الدينامية للتحكم في النفاذ لخدمات أمنية مثل جدران الحماية تمثل تحدياً. ويعود ذلك إلى أن قواعد جدار الحماية تحتاج إلى إضافة دينامية للتصدي لهجمات جديدة على الشبكة.

- وضع سياسة مرعية

ينبغي وضع سياسة بشأن كل مورد شبكي. ولكن يصعب وصف أي من التدفقات هي تدفقات مسموحة وممنوعة ضمن شبكة منظمة محددة تحت الإدارة. وبالتالي، يمكن أن يستعان برؤية مركزية في تحديد السياسات الأمنية لهذه الشبكة.

- آلية النفاذ القائمة على الرزم

لا تكفي آلية النفاذ القائمة على الرزم في الواقع لأن الوحدة الأساسية للتحكم في النفاذ تتمثل عادة في مستخدمين أو تطبيقات. لذلك، يتعين تحديد قواعد مستوى التطبيق وإضافتها إلى خدمة جدار الحماية بواسطة جهة مسؤولة.

2.1.I خدمة المصيدة الجاذبة المركزية

تواجه المصائد الجاذبة التقليدية تحديات في مجالات مثل التكاليف الكبيرة والأداء وإدارة التحكم في النفاذ ووضع سياسة مرعية وآليات نفاذ قائمة على الرزم. وللتعامل مع هذه التحديات، تعرض هذه التوصية إطار خدمة مصيدة جاذبة مركزية قائمة على التوصيل الشبكي المعرَّف بالبرمجيات (SDN). ويمكن إدارة أماكن المصيدة الجاذبة بمرونة بواسطة مخدِّم مركزي. ويمكن استخدام بروتوكولات التوصيل الشبكي المعرَّف بالبرمجيات القائمة من خلال سطوح بينية معيارية بين تطبيقات وبدالات المصيدة الجاذبة.

- التكلفة

تترتب على تشغيل مصائد جاذبة إضافية في الشبكة تكلفة كبيرة بسبب الحاجة إلى استخدام موارد شبكية إضافية مثل مضيفات المصائد الجاذبة. وللتغلب على هذا الإشكال، يمكن إدارة أماكن المصيدة الجاذبة بمرونة بواسطة مخدِّم مركزي.

- الأداء

يعتمد أداء المصائد الجاذبة على قدرة الآلات المضيفة. وتعمل كل مصيدة جاذبة دائماً بنفس الطريقة دون الرجوع إلى ظروف الشبكة أو الهجوم. ويمكن نشر المصائد الجاذبة بشكل متكيف وفقاً لظروف الشبكة أو الهجوم في هذا الإطار.

- إدارة التحكم في النفاذ

نظراً لوجود مئات من موارد الشبكة في شبكة مدارة، فإن التشكيلة الدينامية للمصائد الجاذبة تمثل تحدياً. ويعود ذلك إلى أن أماكن مصيدة جاذبة تحتاج إلى تغيير دينامي للتصدي لهجمات جديدة على الشبكة.

- وضع سياسة مرعية

ينبغي وضع سياسة بشأن كل مورد شبكي. ولكن يصعب تحديد أماكن معينة لمصيدة جاذبة ضد الهجمات المشبوهة حسب ظروف الشبكة والهجوم. وبالتالي، يمكن أن يستعان برؤية مركزية في تحديد السياسات الأمنية لهذه الشبكة.

- آلية نشر مصيدة جاذبة

ينبغي نشر أماكن مصيدة جاذبة بشكل صحيح حسب ظروف الشبكة والهجوم. تحدد خدمة مصيدة جاذبة مركزية تستند إلى التوصيل الشبكي المعرَّف بالبرمجيات (SDN) المكان الأمثل لمراقبة الهجمات والرد عليها في الوقت الفعلي. ويقوم مخدِّم مركزي بتشكيل مصيدة جاذبة مركزياً كهدف للهجوم المقصود.

2.I معايير خدمات الأمن في شبكات الميدان البيني

1.2.I خدمة تخفيف هجوم DDoS المركزية

تدافع خدمة تخفيف هجوم DDoS المركزية عن المخدِّمات ضد هجوم DDoS خارج الشبكات الخاصة، أي من الشبكات العامة. وتصنَّف المخدِّمات ضمن مخدِّمات عديمة الحالة المخزنة (مثل مخدِّمات DNS) ومخدِّمات ذات حالة مخزنة (مثل مخدِّمات شبكة الإنترنت). ويوضح الشكل 8-6 تشكيل خدمة تخفيف هجوم DDoS في شبكة خاصة. ويجري تشكيل البدالات في الشبكة الخاصة في مستويات ميدان تراتبية، أي بدالات المستوى 1، وبدالات المستوى الثاني، وبدالات المستوى – n وهلم جراً، لإقامة خطوط دفاع دينامية مقابل مجموعة متنوعة من هجمات DDoS.

وتواجه خدمة تخفيف هجوم DDoS المركزية تحديات في مجالات مثل التكلفة الكبيرة والأداء وإدارة التحكم في النفاذ ووضع سياسة مرعية وآليات نفاذ قائمة على الرزم. وللتعامل مع هذه التحديات، تعرض هذه التوصية إطار خدمة تخفيف هجوم DDoS مركزية قائمة على التوصيل الشبكي المعرَّف بالبرمجيات (SDN). ويمكن إدارة قواعد تخفيف هجوم DDoS بمرونة بواسطة مخدِّم مركزي. ويمكن استخدام بروتوكولات التوصيل الشبكي المعرَّف بالبرمجيات القائمة من خلال سطوح بينية معيارية بين تطبيقات وبدالات تخفيف هجوم DDoS.

- التكلفة

تمكن إدارة كل مورد شبكي بطريقة مركزية ومرنة بأقل تكلفة بحيث يجري تشكيل البدالات والتعامل معها على مستويات متعددة بواسطة مخدِّم مركزي. وبازدياد ضراوة هجمات DDoS على مخدِّم، تقوم البدالات متعددة المستويات بإسقاطات انتقائية للرزم لتقليل تأثير هجمات DDoS. وبعبارة أخرى، تُسقَط رزم هجوم DDoS المشبوهة مبكراً في بداية مسار التسيير إلى المضيف المتأثر.

- الأداء

كثيراً ما يكون أداء تخفيف هجوم DDoS المركزي أبطأ من سرعة وصلة السطوح البينية لشبكته. وفي الخدمة التقليدية، يحتاج كل مورد شبكي للتحقق من قواعد تخفيف هجوم DDoS دون الرجوع إلى ظروف الشبكة. ولكن يمكن نشر تطبيقات تخفيف هجوم DDoS بشكل متكيف وفقاً لظروف الشبكة في هذا الإطار.

- إدارة التحكم في النفاذ

نظراً لوجود مئات من موارد الشبكة في شبكة مدارة، فإن الإدارة الدينامية للتحكم في النفاذ لخدمات أمنية مثل التخفيف من هجوم DDoS تمثل تحدياً. ويعود ذلك إلى أن قواعد تخفيف هجوم DDoS تحتاج إلى إضافة دينامية للتصدي لهجمات DDoS جديدة على الشبكة.

- وضع سياسة مرعية

ينبغي وضع سياسة بشأن كل مورد شبكي. ولكن يصعب تحديد سياسات معينة لإسقاط الرزم ضد هجمات DDoS حسب ظروف الشبكة. وبالتالي، يمكن أن يستعان برؤية مركزية في تحديد السياسات الأمنية لهذه الشبكة.

- آلية كشف هجوم DDoS

يُكشف هجوم DDoS من خلال التحقق مما إذا كانت طلبات الخدمات من أحد العملاء تأتي في فاصل زمني متوقع أم لا. وتحدد آلية كشف هجوم DDoS احتمال كون الطلبات من عميل هي هجوم DDoS وتقوم بإسقاط انتقائي للطلبات بوتيرة أعلى بالتناسب مع هذا الاحتمال.

2.2.I الخدمة المركزية لإدارة الأجهزة غير القانونية

تواجه الخدمات التقليدية لإدارة الأجهزة غير القانونية تحديات في مجالات مثل التكاليف الكبيرة والأداء وإدارة التحكم في النفاذ ووضع سياسة مرعية وآليات نفاذ قائمة على الرزم. وللتعامل مع هذه التحديات، تعرض هذه التوصية إطار خدمة مركزية لإدارة الأجهزة غير القانونية على أساس التوصيل الشبكي المعرَّف بالبرمجيات (SDN). ويمكن إدارة قواعد إدراج الأجهزة في قائمة سوداء على مستوى العالم. ويمكن استخدام بروتوكولات التوصيل الشبكي المعرَّف بالبرمجيات القائمة من خلال سطوح بينية معيارية بين تطبيقات وبدالات جهاز غير قانوني.

- التكلفة

تعتبر تكلفة تحديث القوائم السوداء لموارد الشبكة مثل المسيِّرات والبوابات والبدالات كبيرة بسبب الحاجة إلى تحديث القوائم السوداء لكل مورد شبكة على حدة. وللتغلب على هذا الإشكال، يمكن إدارة كل مورد شبكي مركزياً بحيث يتعامل مخدِّم مركزي مع خدمة إدارة جهاز غير قانوني واحدة.

- الأداء

بما أن الرزم تُسقَط من الأجهزة المدرجة في القائمة السوداء في بداية مسار التسيير بخلاف خدمة الإدارة التقليدية، يمكن تحسين أداء الخدمة المركزية لإدارة الأجهزة غير القانونية في الممارسة العملية.

- إدارة التحكم في النفاذ

عندما تدار القوائم السوداء محلياً، لا تسهل مزامنة القوائم السوداء الموزعة محلياً نظراً لإمكانية وجود مئات من موارد الشبكة في مختلف البلدان. ويتعين إضافة قواعد الأمن دينامياً بشأن الأجهزة الجديدة غير القانونية.

- وضع سياسة مرعية

ينبغي وضع سياسة لكل مورد من موارد الشبكة. بيد أنه يصعب وصف الأجهزة التي يجب حظرها داخل شبكة أي منظمة بعينها قيد الإدارة. ولذا، قد يساعد وجود رؤية مركزية في تحديد السياسات الأمنية لشبكة كهذه.

- آلية تحديث القائمة السوداء

من الأهمية بمكان الاحتفاظ بقائمة سوداء حديثة للأجهزة غير القانونية. لذلك، يجب على الخدمات التقليدية الحالية تحديث قاعدة بيانات القائمة السوداء بانتظام لمواكبة أحدث المعلومات عن أي أجهزة غير قانونية. في الخدمة المركزية لإدارة الأجهزة غير القانونية، تدار القائمة السوداء مركزياً كقاعدة بيانات منطقية واحدة بواسطة مخدِّم مركزي.

3.2.I خدمة إدارة التحكم في النفاذ

تواجه خدمات إدارة التحكم في النفاذ تحديات في مجالات مثل التكاليف الكبيرة والأداء وإدارة التحكم في النفاذ ووضع سياسة مرعية وآليات نفاذ قائمة على الرزم. وللتعامل مع هذه التحديات، تعرض هذه التوصية خدمة إدارة التحكم في النفاذ على أساس التوصيل الشبكي المعرَّف بالبرمجيات (SDN). وتمكن إدارة قواعد إدراج الأجهزة في قائمة بيضاء على مستوى العالم في خدمات الشبكة الموزَّعة (مثل مراقب التوصيل الشبكي المعرَّف بالبرمجيات، بدالة). ويمكن استخدام بروتوكولات التوصيل الشبكي المعرَّف بالبرمجيات القائمة من خلال سطوح بينية معيارية بين تطبيقات وبدالات إدارة التحكم في النفاذ عبر مراقب التوصيل الشبكي المعرَّف بالبرمجيات.

- التكلفة

تعتبر تكلفة تحديث القوائم البيضاء لموارد الشبكة مثل المسيِّرات والبوابات والبدالات كبيرة بسبب الحاجة إلى تحديث القوائم البيضاء لكل مورد شبكة على حدة. وللتغلب على هذا الإشكال، تمكن إدارة كل مورد شبكي مركزياً بحيث يتعامل مخدِّم مركزي مع خدمة إدارة تحكم في النفاذ واحدة.

- الأداء

بما أن الرزم تُسقَّط من الأجهزة التي لا تملك حقوق نفاذ في بداية مسار التسيير بخلاف خدمة الإدارة التقليدية، يمكن تحسين أداء خدمة إدارة التحكم في النفاذ في الممارسة العملية. بالإضافة إلى ذلك، ستقسَّم المعلومات المتعلقة بحقوق النفاذ وتخزَّن في موارد الشبكة وفق مستوى الأمن الخاص بها.

- إدارة التحكم في النفاذ

عندما تدار القوائم البيضاء محلياً، لا تسهل مزامنتها نظراً لإمكانية وجود مئات من موارد الشبكة في مختلف البلدان. ويتعين نشر قواعد الأمن دينامياً لإرسال حقوق النفاذ الجديدة إلى موارد الشبكة.

- وضع سياسة مرعية

ينبغي وضع سياسة لكل مورد من موارد الشبكة وفق مستوى الأمن الخاص به. ولكن يصعب وصف أجهزة إنترنت الأشياء التي يجب حظرها داخل شبكة أي منظمة بعينها قيد إدارة التحكم في النفاذ. ولذا، قد يساعد وجود رؤية مركزية في تحديد السياسات الأمنية لشبكة كهذه.

- آلية تحديث القائمة البيضاء

من الأهمية بمكان الاحتفاظ بقائمة بيضاء حديثة لحقوق نفاذ أجهزة إنترنت الأشياء. لذلك، يجب على الخدمات التقليدية الحالية تحديث قاعدة بيانات القائمة البيضاء بانتظام لمواكبة أحدث المعلومات عن حقوق نفاذ أجهزة إنترنت الأشياء. وفي خدمة إدارة التحكم في النفاذ، تدار القائمة البيضاء مركزياً كقاعدة بيانات منطقية واحدة بواسطة مخدِّم مركزي. بالإضافة إلى ذلك، يجوز توزيع بعض أجزاء السياسات المرعية على موارد الشبكة.

التذييل II

مثال على كشف رزم البيانات بالمسح

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يتطلب كشف رزم البيانات بالمسح دعماً من أجل اكتشاف بعض الهجمات مثل ملفات الدودة البرمجية والتخفيف منها. ويقوم المسؤول بتشكيل السياسات لكشف بعض رزم التدفق فقط بشكل عشوائي وليس كل رزم التدفق للحصول على أداء أعلى. وينطوي أحد مخططات كشف رزم البيانات بالمسح [b-ICIN SDNSec] على اختيار أول رزم m متتالية من كل تدفق لأداء كشف رزم البيانات بالمسح. ويمكن تصميم هذا المخطط لجميع التدفقات أو لتدفقات تلبي شروطاً معينة حصراً، مثل رزم آتية من عنوان بروتوكول إنترنت (IP) معين المصدر و/أو متجهة إلى مقصد معين.

ويجوز توسيع بروتوكول OpenFlow [b-ONF TS-012]، كأحد تطبيقات السطح البيني للتوصيل الشبكي المعرَّف بالبرمجيات (SDN) المتجهة إلى المستوى الأدنى، من أجل دعم كشف رزم البيانات بالمسح. وتمكن إضافة ميزتين إضافيتين إلى نسق قيد التدفق. ويجب أن ترد هذه التحديثات في وحدة التحكم والبدالات معاً. وتتمثل إحدى هذه الميزات في المخطط الذي يتضمن كشف رزم البيانات بالمسح. وترد الميزة الأخرى في الشرط الذي يصف التدفقات التي تفي بالشروط التي شكلها المسؤول أو التطبيقات. وينبغي عندئذ أن يضاف الإجراء الاختياري (OFPAT_DETECTION) في الفقرة 12.5 من المرجع [b-ONF TS-012] على النحو الموضح في النصوص التالية بخط مائل: *إجراء اختياري: إجراء كشف يعيد تسيير رزمة إلى منفذ OpenFlow ثم إلى أجهزة أمنية (من قبيل FW، IDP، DPI، وما إلى ذلك.) لمواصلة كشف البيانات بالمسح*. وهذا الإجراء الجديد يشبه الإجراء OFPAT_OUTPUT في بروتوكول OpenFlow. وأخيراً، ينبغي تحديث هياكل الإجراءات في الفقرة 4.2.7 في المرجع [b-ONF TS-012] على النحو الموضح فيما يلي بالنصوص المكتوبة بخط مائل:

```
enum ofp_action_type {
OFPAT_OUTPUT = 0,                          /* Output to switch port. */
OFPAT_DETECTION = XX (a given number),     /*Output to switch port */
OFPAT_COPY_TTL_OUT = 11,      /* Copy TTL "outwards" – from
                                 next-to-outermost to outermost */
OFPAT_COPY_TTL_IN = 12,       /* Copy TTL "inwards" – from
                                outermost to next-to-outermost */
OFPAT_SET_MPLS_TTL = 15,      /* MPLS TTL */
OFPAT_DEC_MPLS_TTL = 16,      /* Decrement MPLS TTL */
OFPAT_PUSH_VLAN = 17,         /* Push a new VLAN tag */
OFPAT_POP_VLAN = 18,          /* Pop the outer VLAN tag */
OFPAT_PUSH_MPLS = 19,         /* Push a new MPLS tag */
OFPAT_POP_MPLS = 20,          /* Pop the outer MPLS tag */
OFPAT_SET_QUEUE = 21,          /* Set queue id when outputting to a port */
OFPAT_GROUP = 22,              /* Apply group. */
OFPAT_SET_NW_TTL = 23,         /* IP TTL. */
OFPAT_DEC_NW_TTL = 24,          /* Decrement IP TTL. */
OFPAT_SET_FIELD = 25,          /*Set a header field using OXM TLV format*/
OFPAT_PUSH_PBB = 26,            /* Push a new PBB service tag (I-TAG) */
OFPAT_POP_PBB = 27,           /* Pop the outer PBB service tag (I-TAG) */
OFPAT_EXPERIMENTER = 0xffff
};
A Detection action uses the following structure and fields:
/*Action structure for OFPAT_DETECTION which sends packets out 'port'.*/
struct ofp_action_detection {
uint16_t type;                  /* OFPAT_DETECTION. */
uint16_t len;                   /* Length is 16. */
uint32_t port;                  /* Output port. */
uint16_t schema;                /* One possible schema is: to select the first m
                                 consecutive packets from each flow. */
uint32_t condition;            /* One possible condition: packets
                                of the flow to a certain destination. */
};
OFP_ASSERT(sizeof(struct ofp_action_output) == 10);
```

التذييل III

معمارية تنفيذ خدمات الأمن القائمة على التوصيل الشبكي المعرَّف بالبرمجيات (SDN)

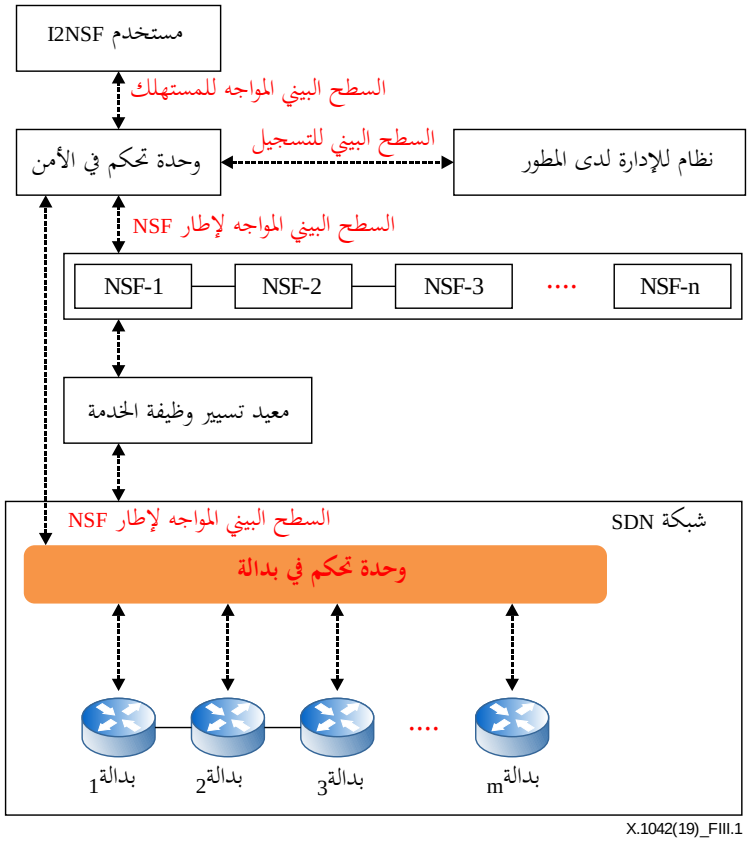
(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.III السطح البيني لإطار وظيفة أمن الشبكة (I2NSF) مع التوصيل الشبكي المعرَّف بالبرمجيات (SDN) لدى فريق مهام هندسة الإنترنت (IETF)

1.1.III نظرة عامة

تقدم هذه الفقرة السطح البيني لإطار وظيفة أمن الشبكة (I2NSF) مع التوصيل الشبكي المعرَّف بالبرمجيات (SDN) لدى فريق مهام هندسة الإنترنت (IETF) في خدمات الأمن القائمة على الحوسبة السحابية مثل جدران الحماية والتفتيش العميق للرزم ووظائف تخفيف هجوم DDoS. ويفعِّل التوصيل الشبكي المعرَّف بالبرمجيات إمكانية إنفاذ بعض قواعد اصطفاء الرزم في بدالات الشبكة من خلال التحكم في قواعد إعادة تسيير الرزم الخاصة بها. وبالاستفادة من هذه القدرة على التوصيل الشبكي المعرَّف بالبرمجيات، يمكن تحقيق الإنفاذ الأمثل لخدمة الأمن في إطار I2NSF.

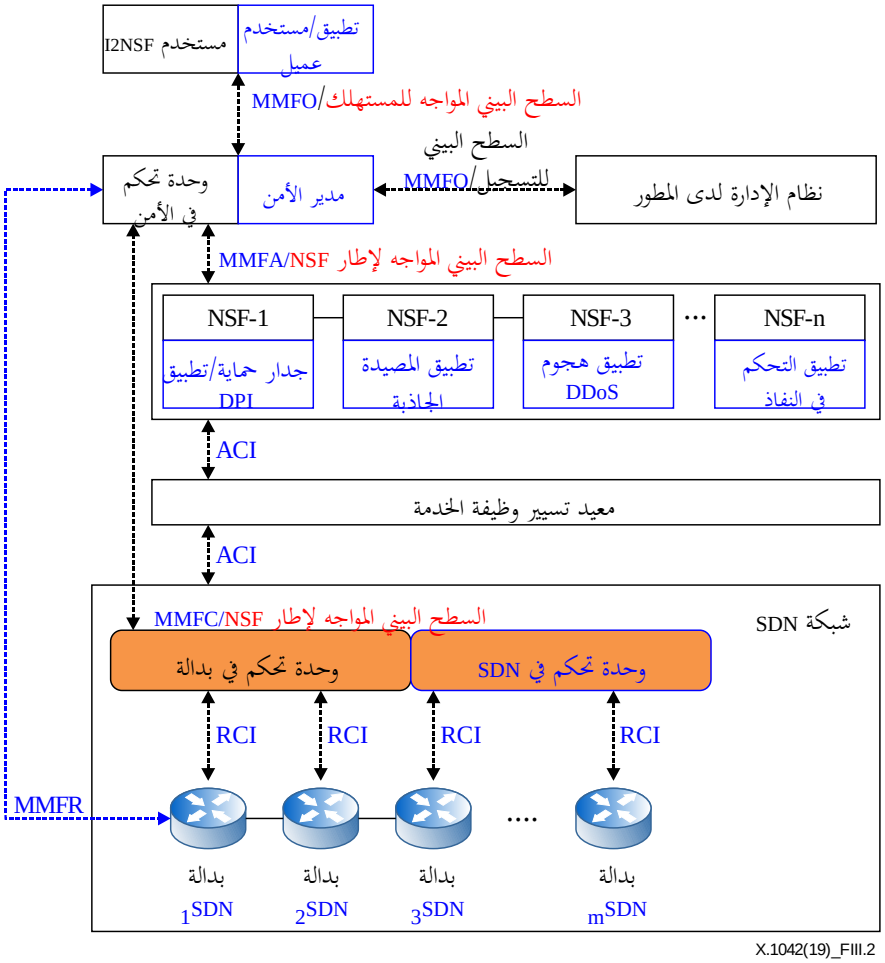
ويوضح الشكل 1.III إطار I2NSF [b-IETF RFC 8329] بشبكات التوصيل الشبكي المعرَّف بالبرمجيات (SDN) لدعم خدمات الأمن القائمة على الشبكة. وفي هذا الإطار، ينقسم تنفيذ قواعد السياسة الأمنية بين بدالات التوصيل الشبكي المعرَّف بالبرمجيات ووظائف أمن الشبكة (NSFs). وهنا، يُستخدم بروتوكول NETCONF ولغة النمذجة YANG.



الشكل 1-III – السطح البيني لإطار وظيفة أمن الشبكة لدى فريق مهام هندسة الإنترنت (IETF)

2.1.III مقارنة بين معماريتي فريق مهام هندسة الإنترنت وقطاع تقييس الاتصالات

يوضح الشكل 2.III مقارنة إطار I2NSF باستخدام التوصيل الشبكي المعرَّف بالبرمجيات (SDN) ومعمارية قطاع تقييس الاتصالات. وتظهر مكونات قطاع تقييس الاتصالات باللون الأزرق.

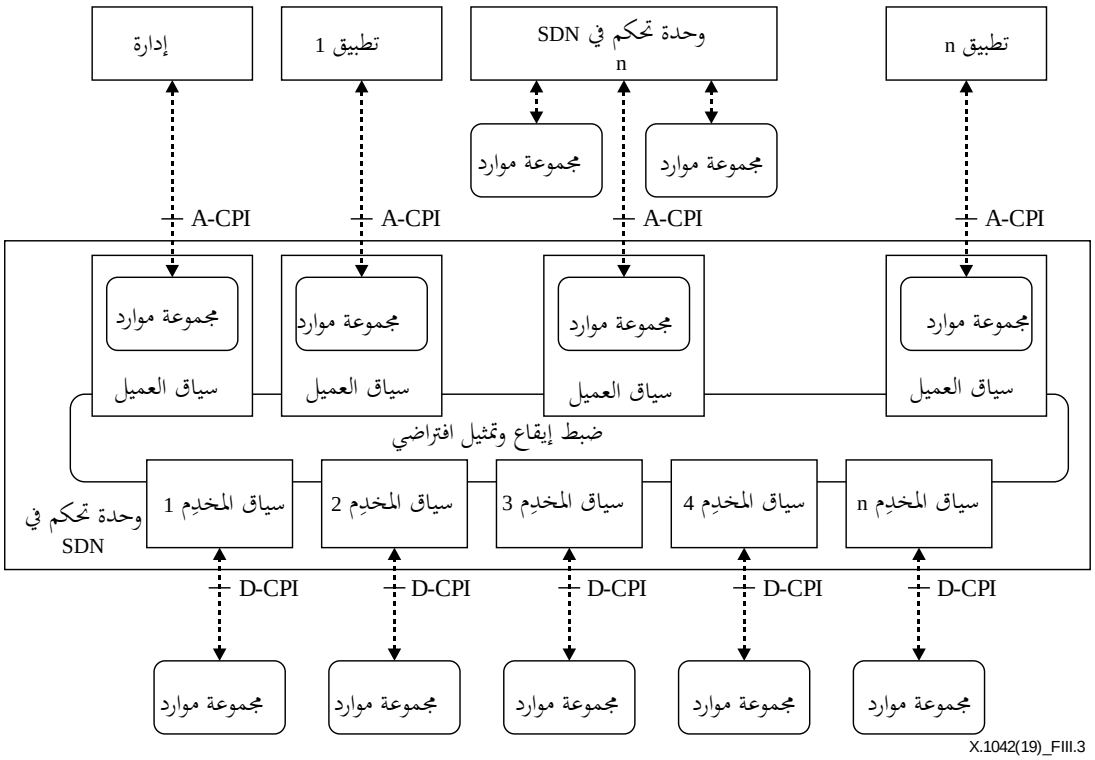


الشكل 2-III – مقارنة بين معماريتي فريق مهام هندسة الإنترنت وقطاع تقييس الاتصالات

2.III معمارية التوصيل الشبكي المعرَّف بالبرمجيات (SDN) في مؤسسة التوصيل الشبكي المفتوح (ONF)

1.2.III نظرة عامة

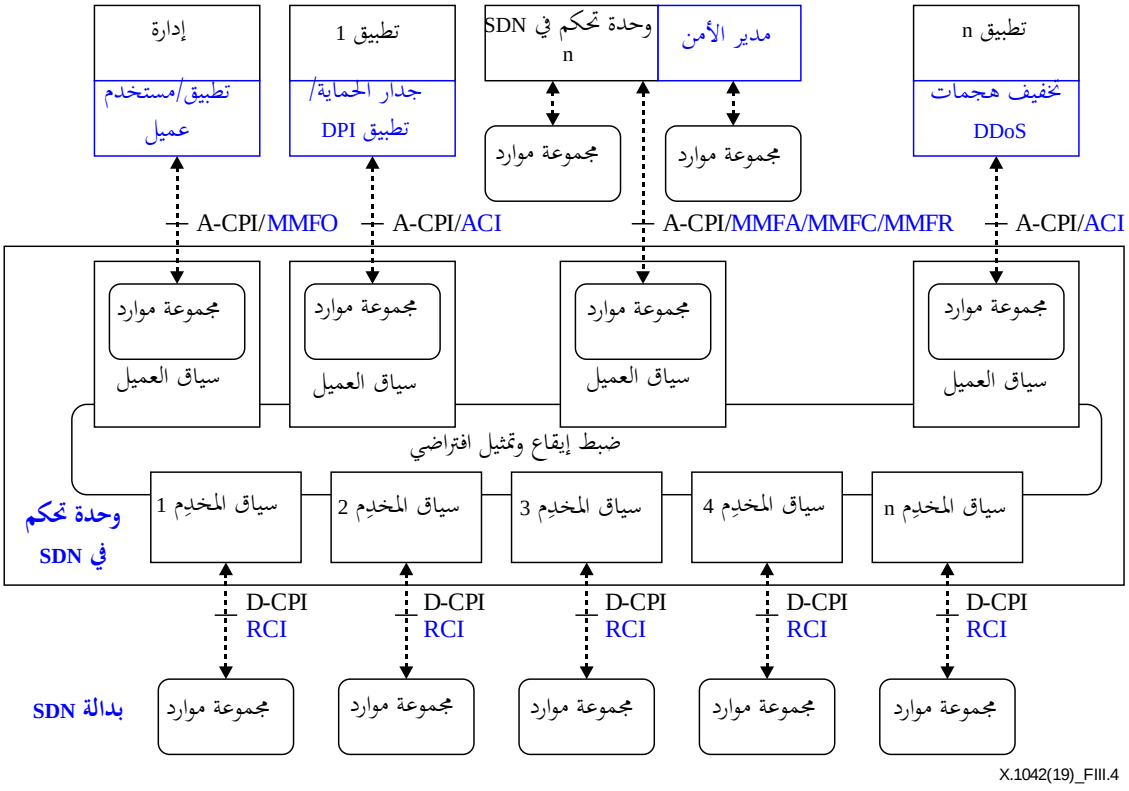
تقدم هذه الفقرة معمارية التوصيل الشبكي المعرَّف بالبرمجيات (SDN) في مؤسسة التوصيل الشبكي المفتوح (ONF). ويبين الشكل 3.III معمارية التوصيل الشبكي المعرَّف بالبرمجيات (SDN) الواردة في المرجع [b-ONF TR-521]. وفي الشكل 3.III، تُمذج التوصيل الشبكي المعرَّف بالبرمجيات كمجموعة من علاقات العميل والمخدِّم بين وحدات التحكم في التوصيل الشبكي المعرَّف بالبرمجيات والكيانات الأخرى التي يمكن أن تكون نفسها وحدات تحكم في التوصيل الشبكي المعرَّف بالبرمجيات. وفي دورها كمخدِّم، يمكن أن تقدم وحدة التحكم في التوصيل الشبكي المعرَّف بالبرمجيات خدمات إلى أي عدد من العملاء، بينما يمكن لوحدة التحكم هذه العاملة كعميل أن تستدعي خدمات من أي عدد من المخدِّمات. وطالما أنها تُظهر سلوكاً مناسباً للسطح البيني، فإن التفاصيل الداخلية للكيانات المغايرة لوحدات التحكم في التوصيل الشبكي المعرَّف بالبرمجيات تقع خارج مجال تطبيق هذه المعمارية. وهنا، يُستخدم بروتوكول openflow.



الشكل III-3 معمارية التوصيل الشبكي المعرَّف بالبرمجيات (SDN) في مؤسسة التوصيل الشبكي المفتوح (ONF)

2.2.III مقارنة بين معماريتي مؤسسة التوصيل الشبكي المفتوح وقطاع تقييس الاتصالات

يوضح الشكل 4.III مقارنة بين معماريتي مؤسسة التوصيل الشبكي المفتوح (ONF) وقطاع تقييس الاتصالات (ITU-T). وتظهر مكونات قطاع تقييس الاتصالات باللون الأزرق.



الشكل III-4 مقارنة بين معماريتي مؤسسة التوصيل الشبكي المفتوح وقطاع تقييس الاتصالات

بيبليوغرافيا

[b-ITU-T X.812] Recommendation ITU-T X.812 (1995) | ISO/IEC 10181-3:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework.*

[b-ITU-T X.1252] Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

[b-ICIN SDNSec] Hu, Z., Wang, M., Yan, X., Yin, Y., Luo, Z. (2015). A comprehensive security architecture for SDN. In: *18th International Conference on Intelligence in Next Generation Networks*, pp 30-37. New York, NY: IEEE. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7073803

[b-IETF RFC 8329] IETF RFC 8329 (2018), *Framework for interface to network security functions*. https://tools.ietf.org/html/rfc8329.

[b-ONF TR-521] Open Networking Foundation TR-521 (2016), *SDN architecture*. https://www.opennetworking.org/wp-content/uploads/2014/10/TR-521_SDN_Architecture_issue_1.1.pdf

[b-ONF TS-012] Open Networking Foundation TS-012 (2013). *OpenFlow switch specification V.1.4.0*.https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-spec-v1.4.0.pdf

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	مبادئ التعريفة والمحاسبة والقضايا الاقتصادية والسياساتية المتصلة بالاتصالات/تكنولوجيا المعلومات والاتصالات على الصعيد الدولي
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	البيئة وتكنولوجيا المعلومات والاتصالات، وتغير المناخ، والمخلفات الإلكترونية، وكفاءة استخدام الطاقة، وإنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير، والقياسات والاختبارات المرتبطة بهما
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التليماتية
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، والجوانب الخاصة ببروتوكول الإنترنت وشبكات الجيل التالي وإنترنت الأشياء والمدن الذكية
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2019