Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1042

(01/2019)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité de l'information et des réseaux – Sécurité des réseaux

Services de sécurité utilisant les réseaux pilotés par logiciel

Recommandation UIT-T X.1042

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	**X.1030–X.1049**
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1360–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1389
Sécurité de la technologie des registres distribués	X.1400–X.1429
Sécurité de la technologie des registres distribués	X.1430–X.1449
Protocoles de sécurité (2)	X.1450–X.1459
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en oeuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699

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

Recommandation UIT-T X.1042

Services de sécurité utilisant les réseaux pilotés par logiciel

Résumé

La Recommandation UIT-T X.1042 porte sur la protection des ressources de réseau au moyen de services de sécurité fondés sur les réseaux pilotés par logiciel (SDN). Elle commence par établir une classification des ressources de réseau pour les services de sécurité fondés sur les réseaux SDN: application SDN, contrôleur SDN, commutateur SDN et gestionnaire de la sécurité (SM). Elle définit ensuite les services de sécurité fondés sur les réseaux SDN.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T X.1042	30-01-2019	17	11.1002/1000/13803

Mots clés

Contrôle d'accès, attaque DDoS, pare-feu, leurre, réseau piloté par logiciel (SDN), scénarios de sécurité.

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

AVANT-PROPOS

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

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

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

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

NOTE

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

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

DROITS DE PROPRIÉTÉ INTELLECTUELLE

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

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

TABLE DES MATIÈRES

Recommandation UIT-T X.1042

Services de sécurité utilisant les réseaux pilotés par logiciel

1 Domaine d'application

La présente Recommandation porte sur la protection des ressources de réseau au moyen de services de sécurité fondés sur les réseaux pilotés par logiciel (SDN). Elle traite de:

– la classification des ressources de réseau qui peuvent être protégées par des services de sécurité fondés sur les réseaux SDN;

– la définition de services de sécurité fondés sur les réseaux SDN;

– la spécification de la mise en oeuvre de services de sécurité fondés sur les réseaux SDN.

La protection des ressources de réseau (par exemple, les routeurs, commutateurs, pare-feu et systèmes de détection des intrusions) par des services de sécurité fondés sur les réseaux SDN comprend les éléments suivants:

– une réaction rapide en cas de nouvelles attaques de réseau (par exemple, des vers ou des attaques par déni de service réparti (DDoS));

– la constitution de réseaux privés visant à atténuer les effets des attaques de réseau sophistiquées;

– un système de défense automatique contre les attaques de réseau sans intervention des administrateurs du réseau;

– une attribution de ressources dynamique en fonction de la charge du réseau.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toute recommandation ou autre référence étant sujette à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des recommandations et autres références énumérées ci-dessous. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T Y.3300] Recommandation UIT-T Y.3300 (2014), *Cadre des réseaux pilotés par logiciel*.

[UIT-T Y.3301] Recommandation UIT-T Y.3301 (2016), *Exigences fonctionnelles des réseaux pilotés par logiciel*.

[UIT-T Y.3302] Recommandation UIT-T Y.3302 (2017), *Architecture fonctionnelle des réseaux pilotés par logiciel*.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation emploie les termes suivants définis ailleurs:

3.1.1 réseau piloté par logiciel [UIT-T Y.3300]: ensemble de techniques permettant de programmer, d'orchestrer, de contrôler et de gérer les ressources de réseau de manière directe, ce qui facilite la mise au point, la fourniture et le fonctionnement de services de réseau de façon dynamique et modulable.

3.1.2 contrôle d'accès [b-UIT-T X.1252]: procédure utilisée pour déterminer si l'accès à des ressources, fonctionnalités, services ou informations devrait être accordé à une entité, compte tenu des règles préétablies et de l'autorité ou des droits spécifiques associés à l'entité requérante.

3.1.3 politique de contrôle d'accès [b-UIT-T X.812]: ensemble des règles définissant les conditions dans lesquelles un accès peut être accordé.

3.1.4 règles de politique de contrôle d'accès [b-UIT-T X.812]: règles de politique de sécurité concernant la fourniture du service de contrôle d'accès.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 ressource de réseau: dispositif assurant l'acheminement des paquets dans un système en réseau.

NOTE – Les ressources de réseau comprennent les commutateurs, les routeurs, les passerelles et les points d'accès WiFi.

3.2.2 pare-feu: dispositif ou service situé à la jonction de deux segments de réseau contrôlant chaque paquet qui tente de franchir la limite. Il rejette aussi tout paquet qui n'est pas conforme à certains critères, par exemple la présence de numéros de port ou d'adresses IP non autorisés.

NOTE – Les services de pare-feu peuvent être dissociés des dispositifs physiques et du fonctionnement en tant qu'application.

3.2.3 leurre: mécanisme de sécurité informatique destiné à servir de leurre pour les auteurs de cyberattaques. Ce mécanisme est utilisé pour détecter ou détourner les attaques de leur cible légitime et pour recueillir des données relatives aux attaques subies. Le terme "leurre" est inspiré du comportement consistant à attirer les auteurs d'attaques vers un emplacement (la cible de l'attaque) faisant office de piège.

3.2.4 service centralisé de pare-feu: service permettant d'établir des règles de politique de contrôle d'accès et de les distribuer aux ressources de réseau afin d'assurer l'efficacité de la gestion du pare-feu. Ces règles peuvent être gérées de façon dynamique par un serveur centralisé. Un réseau piloté par logiciel (SDN) peut fonctionner comme un service centralisé de pare-feu au moyen d'une interface normalisée entre les applications de pare-feu et les ressources de réseau.

3.2.5 service centralisé d'atténuation des effets des attaques DDoS: service permettant d'établir des règles de politique de contrôle d'accès et de les distribuer aux ressources de réseau afin d'assurer l'efficacité de l'atténuation des effets des attaques par déni de service réparti (DDOS). Ces règles peuvent être gérées de façon dynamique par un serveur centralisé. Un réseau piloté par logiciel (SDN) peut fonctionner comme un service centralisé d'atténuation des effets des attaques DDoS au moyen d'une interface normalisée entre les applications d'atténuation des effets des attaques DDoS et les ressources de réseau.

3.2.6 service centralisé de leurre: service permettant d'établir des règles de politique de contrôle d'accès et de les distribuer aux ressources de réseau afin de permettre la configuration dynamique du leurre. Ces règles peuvent être gérées de façon dynamique par un serveur centralisé. Un réseau piloté par logiciel (SDN) peut fonctionner comme un service centralisé de leurre au moyen d'une interface normalisée entre les applications de leurre et les ressources de réseau.

3.2.7 service centralisé de gestion des dispositifs illicites: service permettant d'établir des règles de politique de contrôle d'accès et de les distribuer aux ressources de réseau afin d'inscrire les dispositifs illicites sur une liste noire. Ces règles peuvent être gérées de façon dynamique et globale par un serveur centralisé. Un réseau piloté par logiciel (SDN) peut fonctionner comme un gestionnaire des dispositifs illicites à l'échelle du réseau au moyen d'une interface normalisée entre les applications de gestion des dispositifs illicites et les ressources de réseau.

NOTE – Un critère concernant un dispositif illicite ne relève pas du domaine d'application de la présente Recommandation. Un exemple de dispositif illicite peut être déterminé sur la base du système mondial d'identification unique.

3.2.8 service de gestion du contrôle d'accès: service permettant d'établir des politiques de droit d'accès et de les distribuer aux ressources de réseau pour la liste blanche de dispositifs de l'Internet des objets (IoT). Ces politiques peuvent être gérées de façon dynamique et globale par un serveur centralisé. Un réseau piloté par logiciel (SDN) peut fonctionner comme un gestionnaire de dispositifs IoT à l'échelle du réseau au moyen d'une interface normalisée entre les applications de gestion du contrôle d'accès et les ressources de réseau.

NOTE – La spécification d'une composition hiérarchique des politiques d'accès ne relève pas du domaine d'application de la présente Recommandation. Ces politiques d'accès peuvent être constituées et subdivisées en fonction du niveau de sécurité des ressources de réseau et distribuées aux ressources de réseau.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ACI interface application-commande (*application control interface*)

ACM gestion du contrôle d'accès (*access control management*)

AL-MSO prise en charge et orchestration de la gestion de la couche application (*application layer management support and orchestration*)

ALM gestion de la couche application (*application layer management*)

BSS système d'appui aux activités (*business support system*)

CL-AS prise en charge des applications de la couche commande (*control layer application support*)

CL-CLS service de couche commande de la couche commande (*control layer control layer services*)

CL-MSO prise en charge et orchestration de la gestion de la couche commande (*control layer management support and orchestration*)

CL-RA représentation abstraite des ressources de la couche commande (*control layer resource abstraction*)

CLM gestion de la couche commande (*control layer management*)

DDoS déni de service distribué (*distributed denial-of-service*)

DNS service de noms de domaine (*domain name service*)

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

I2NSF interface avec la fonction de sécurité de réseau (*interface to network security function*)

IoT Internet des objets (*Internet of things*)

IP Protocole Internet (*Internet Protocol*)

MAC commande d'accès au support (media access control)

MMF fonction de gestion multicouche (*multi-layer management function*)

MMFA fonction de gestion multicouche – couche application (*multi-layer management function application layer*)

MMFC fonction de gestion multicouche – couche commande (*multi-layer management function control layer*)

MMFO orchestration des fonctions de gestion multicouche OSS/BSS (*multi-layer management function orchestration OSS/BSS*)

MMFR fonction de gestion multicouche – couche ressources (*multi-layer management function resource layer*)

NSF fonction de sécurité de réseau (*network security function*)

OSS système d'appui à l'exploitation (*operation support system*)

RCI interface ressources-commande (*resource control interface*)

RLM gestion de la couche ressources (*resource layer management*)

RL-MS prise en charge de la gestion de la couche ressources (*resource layer management support*)

SDN réseau piloté par logiciel (*software-defined networking*)

SDN-AL réseau piloté par logiciel – couche application (*software-defined networking – application layer*)

SDN-CL réseau piloté par logiciel – couche commande (*software-defined networking – control layer*)

SDN-RL réseau piloté par logiciel – couche ressources (*software-defined networking – resource layer*)

SIP protocole d'ouverture de session (*session initiation protocol*)

SM gestionnaire de la sécurité (*security manager*)

TCP protocole de commande de transmission (*transmission control protocol*)

VoIP téléphonie utilisant le protocole Internet (*voice over Internet protocol*)

VoLTE téléphonie utilisant la technologie LTE (évolution à long terme) (*voice over long term evolution*)

5 Conventions

Dans la présente Recommandation:

L'expression "il est obligatoire" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "il est recommandé" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

L'expression "il est interdit" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

L'expression "peut, à titre d'option" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Ces mots n'impliquent pas que la mise en oeuvre du vendeur doit incorporer l'option et que la caractéristique peut éventuellement être activée par l'opérateur du réseau/le fournisseur de service. Ils signifient plutôt que le fabricant peut incorporer la caractéristique à titre facultatif et revendiquer néanmoins la conformité avec la spécification.

6 Vue d'ensemble de l'architecture fonctionnelle des réseaux SDN

On trouvera dans le présent paragraphe une description de l'architecture de référence de haut niveau des services de sécurité (par exemple, les pare-feu et l'atténuation des effets des attaques DDoS) utilisant l'architecture de haut niveau des réseaux SDN de la Recommandation [UIT-T Y.3300], y compris les services centralisés de pare-feu et d'atténuation des effets des attaques DDoS.

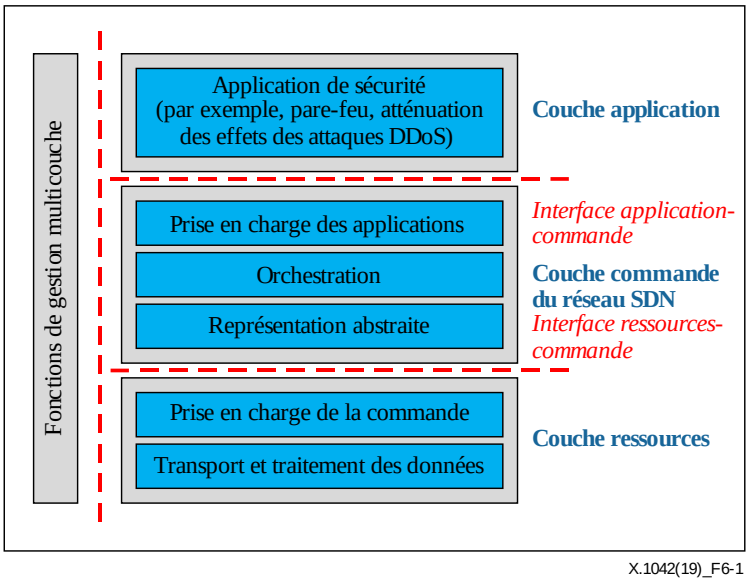


Figure 6-1 – Architecture de haut niveau des services de sécurité fondés sur les réseaux SDN

Comme indiqué dans la Figure 6-1, les applications des services de sécurité (par exemple, les services de pare-feu, d'atténuation des effets des attaques DDoS et de leurre) sont exécutées au-dessus de l'architecture SDN. Lorsqu'un utilisateur ou un administrateur (par exemple, la gestion de la couche application (ALM) dans la Figure 6-2) met en oeuvre des politiques de sécurité pour les services de sécurité via l'interface d'une application, le contrôleur SDN génère les règles de contrôle d'accès correspondantes qui permettent de répondre à ces politiques de sécurité de façon rapide et autonome. Conformément aux règles de contrôle d'accès ainsi générées, les ressources de réseau telles que les commutateurs SDN agissent de façon à atténuer les effets des attaques de réseau, par exemple en abandonnant les paquets qui contiennent des formes suspectes.

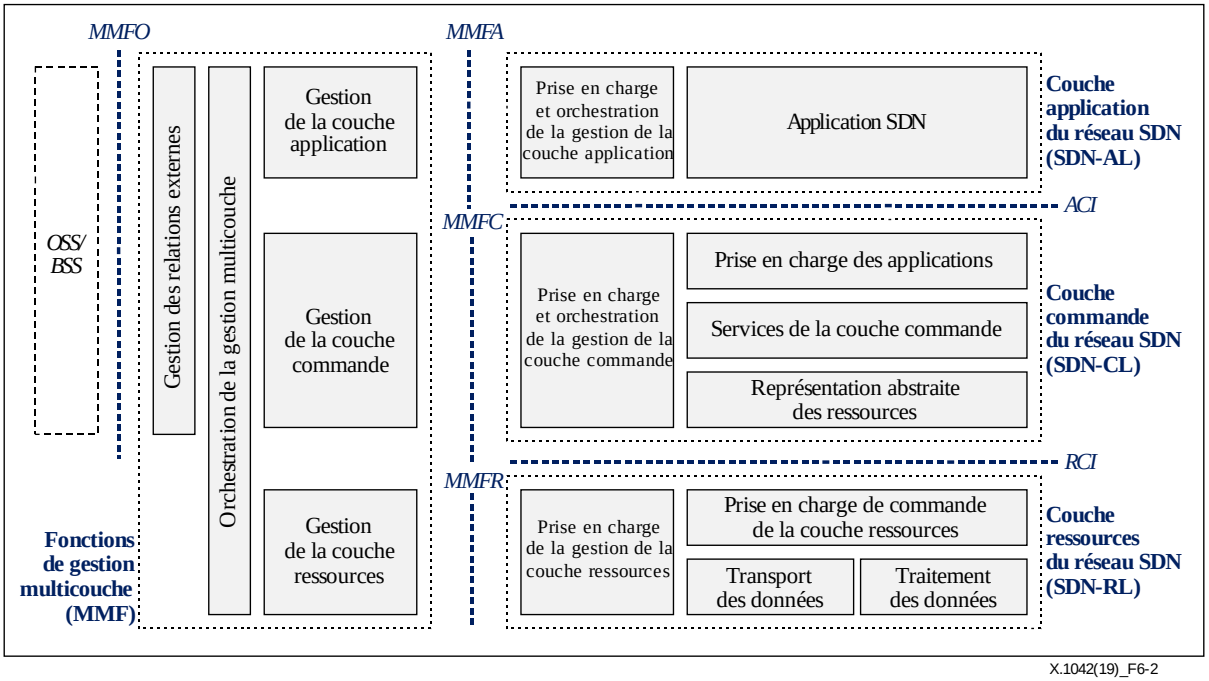
La Figure 6-2 illustre l'architecture fonctionnelle des réseaux SDN décrite dans la Recommandation [UIT-T Y.3302], inspirée de l'architecture de haut niveau des réseaux SDN.

– Couche application – réseau piloté par logiciel (SDN-AL): La couche SDN-AL est constituée du composant fonctionnel de prise en charge et d'orchestration ALM (AL-MSO) et des nombreux composants fonctionnels des applications SDN [UIT-T Y.3302]. L'AL-MSO interagit avec le composant fonctionnel ALM dans la fonction de gestion multicouche (MMF) par l'intermédiaire du point de référence de la fonction de gestion multicouche de la couche application (MMFA) pour prendre en charge la gestion des applications SDN et pour permettre la coordination des opérations de gestion dans toutes les sous-couches SDN. Les applications SDN interagissent avec la couche commande – réseau piloté par logiciel (SDN-CL) par l'intermédiaire du point de référence de l'interface application-commande (ACI) en demandant à la couche SDN-CL d'adapter automatiquement le comportement et les propriétés des ressources de réseau. Les applications SDN utilisent la vue abstraite et le statut des ressources de réseau, qui sont fournis par la couche SDN-CL au moyen de modèles d'informations et de données transmis par le point de référence ACI. En fonction des cas d'utilisation des réseaux SDN (par exemple, entre des centres de données différents ou au

sein d'un même centre de données, dans des réseaux mobiles, dans des réseaux d'accès), différentes interfaces ACI peuvent, à titre d'option, être définies. On suppose que les interfaces ACI utilisent des interfaces de programmation d'application ouvertes.

– SDN-CL: La couche SDN-CL est constituée de la prise en charge et de l'orchestration de la gestion (CL-MSO), de la prise en charge des applications de la couche commande (CL-AS), des services de couche commande de la couche commande (CL-CLS) et de la représentation abstraite des ressources de la couche commande (CL-RA). La couche SDN-CL fournit des moyens programmables de commander le comportement des ressources SDN, par exemple les ressources relatives au transport et au traitement des données, selon les demandes de la couche SND-AL et des politiques de la fonction MMF. La couche SDN-CL agit sur des ressources fournies par la couche ressources du réseau piloté par logiciel (SDN-RL) et délivre une vue abstraite du réseau à la couche SDN-AL. La couche SDN-CL interagit avec la couche SDN-RL par l'intermédiaire d'un point de référence de l'interface ressources-commande (RCI), avec un composant fonctionnel de gestion de la couche commande (CLM) dans la fonction MMF utilisant le point de référence de la fonction de gestion multicouche de la couche commande (MMFC). Elle interagit aussi avec la couche SDN-AL au moyen d'un point de référence ACI. La CL-MSO peut demander que la fonction MMF délègue certaines fonctions de gestion. La fonction MMF fournit des fonctionnalités relatives à la gestion des fonctionnalités de la couche SDN-CL par l'intermédiaire du point de référence MMFC.

– Couche SDN-RL: La couche SDN-RL est constituée de la prise en charge de la gestion de la couche ressources (RL-MS), de la prise en charge de commande de la couche ressources, du traitement des données de la couche ressources et du transport des données de la couche ressources. Les éléments du réseau physique ou virtuel réalisent le transport ou le traitement des paquets de données dans la couche SDN-RL, conformément aux décisions de la couche SDN-CL. Les informations relatives à la mise en place de politiques (y compris les informations de configuration) qui découlent des décisions de la couche SDN-CL, ainsi que les informations concernant les ressources de réseau, sont échangées par l'intermédiaire du point de référence RCI. Les informations échangées au moyen de l'interface RCI comprennent les informations de commande fournies par la couche SDN-CL à la couche SDN-RL, par exemple pour la configuration d'une ressource de réseau ou pour l'établissement de politiques, ainsi que les informations concernant les notifications envoyées par la couche SDN-RL dès lors que la modification d'une ressource de réseau est détectée (si cette information est disponible). La RL-MS fournit une description des ressources, c'est-à-dire le fabricant, la version du logiciel et leur statut (par exemple, la charge de l'unité centrale de traitement, la mémoire vive utilisée ou le stockage). Elle peut comporter un agent de gestion qui réalise certaines opérations de gestion locales dans la mesure où elles lui ont été déléguées par la fonction MMF. La fonction MMF fournit des fonctionnalités relatives à la gestion des fonctionnalités de la couche SDN-RL par l'intermédiaire du point de référence de la fonction de gestion multicouche de la couche ressource (MMFR).



BSS: système d'appui aux activités; MMFO: fonction de gestion multicouche OSS/BSS; OSS: système d'appui à l'exploitation

Figure 6-2 – Architecture fonctionnelle des réseaux SDN [UIT-T Y.3302]

7 Classification des ressources de réseau

On trouvera dans le présent paragraphe la définition de quatre ressources de réseau pour des services de sécurité utilisant les réseaux SDN, sur la base de la Figure 6-2:

1) Application SDN: service qui transmet par programme, de manière explicite et directe, ses exigences relatives au réseau ainsi que le comportement souhaité de celui-ci au contrôleur SDN par l'intermédiaire d'une interface montante telle que l'interface ACI de la Figure 6-2. En outre, les applications SDN peuvent avoir besoin d'une vue abstraite du réseau pour mener à bien leur processus de prise de décision interne. A titre d'exemple, les services de pare-feu, de leurre, d'atténuation des effets des attaques DDoS et de gestion des dispositifs illicites peuvent être fournis en tant qu'application. Ces applications SDN doivent obligatoirement interagir avec l'ALM par l'intermédiaire de l'AL-MSO pour la gestion des dérangements, de la configuration, de la comptabilité, de la qualité de fonctionnement et de la sécurité. De plus, ces applications établissent des règles d'accès; elles doivent donc obligatoirement interagir aussi avec la couche SDN-CL par l'intermédiaire des interfaces ACI pour que ces règles d'accès soient mises en oeuvre.

2) Contrôleur SDN: entité centralisée sur le plan logique chargée de i) convertir les exigences émanant des applications SDN pour les commutateurs SDN; et ii) de fournir des vues abstraites du réseau aux applications, accompagnées d'informations utiles sur le réseau, par exemple des statistiques relatives au trafic et des événements. En d'autres termes, un contrôleur SDN crée des entrées de flux sur la base des règles d'accès qu'il obtient des applications SDN. Par conséquent, le contrôleur SDN doit obligatoirement interagir avec la CLM, les applications SDN et la couche SDN-RL.

3) Commutateur SDN: programme logiciel ou un dispositif matériel qui achemine des paquets dans un environnement SDN. Les commutateurs SDN ont la possibilité de stocker les règles relatives à l'acheminement des paquets gérées par un contrôleur SDN par l'intermédiaire d'une interface descendante telle que l'interface RCI de la Figure 6-2. Par conséquent, le commutateur SDN doit obligatoirement interagir avec la gestion de la couche ressource (RLM) et la couche SDN-CL.

4) Gestionnaire de la sécurité (SM): fonction ALM qui transmet les politiques de sécurité à une application SDN. Le gestionnaire de la sécurité doit donc obligatoirement interagir avec les applications SDN par l'intermédiaire de l'AL-MSO. La Figure 7-1 illustre l'emplacement des ressources de réseau de la Figure 6-2. Ces ressources de réseau doivent obligatoirement respecter les exigences de la Recommandation [UIT-T Y.3301].

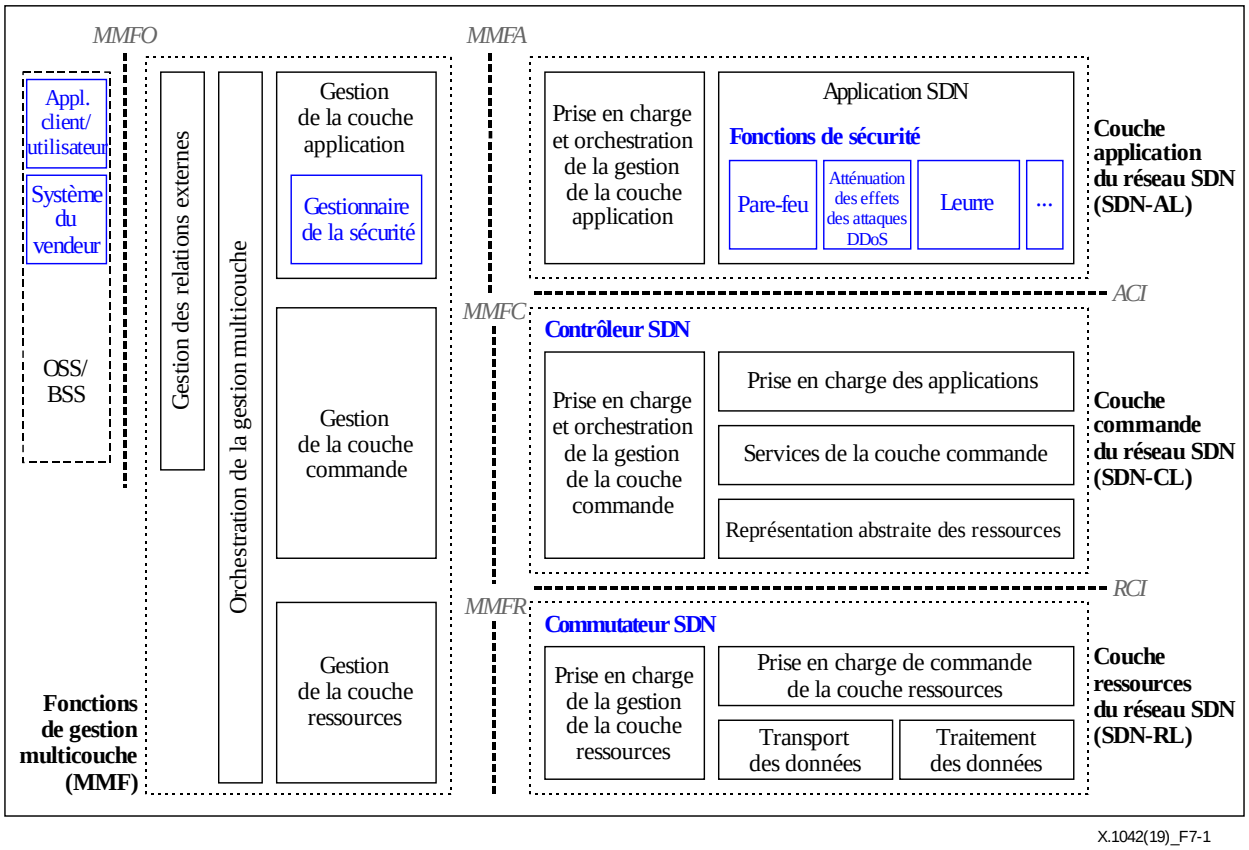


Figure 7-1 – Ressources de réseau dans les services de sécurité fondés sur les réseaux SDN

8 Services de sécurité fondés sur les réseaux SDN

Le présent paragraphe décrit les services de sécurité fondés sur les réseaux SDN dans deux types de réseaux: i) les réseaux intradomaine, par exemple, les services centralisés de pare-feu et de leurre; et ii) les réseaux interdomaines, par exemple, les services centralisés d'atténuation des effets des attaques DDoS et de gestion des dispositifs illicites. Dans la présente Recommandation, on entend par domaine un groupe de ressources de réseau qui est administré selon des règles et procédures communes.

8.1 Service centralisé de pare-feu

8.1.1 Principe de base d'un service centralisé de pare-feu

On trouvera dans le présent paragraphe la description du principe de base d'un service centralisé de pare-feu. Ce type de service peut gérer des ressources de réseau de sorte que les règles de pare-feu puissent être gérées de manière flexible. Comme le montre la Figure 8-1, un pare-feu centralisé gère des commutateurs SDN, dans lesquels il est possible d'insérer ou de supprimer des règles de pare-feu.

NOTE – Il est facile de convertir une stratégie de filtrage des paquets provenant de l'application de pare-feu en un tableau de flux au moyen du contrôleur. Toutefois, un protocole entre le contrôleur et les commutateurs (par exemple, les protocoles OpenFlow et NETCONF) n'est actuellement capable d'établir des correspondances jusqu'à la couche de protocole de commande de transmission (TCP). Il n'y a pas de champ correspondant permettant d'indiquer les informations d'identification d'un paquet de données au-dessus de la

couche TCP. Par conséquent, il est impossible de mettre en oeuvre une stratégie de pare-feu permettant d'identifier les informations au-dessus de la couche TCP sans changer le protocole.

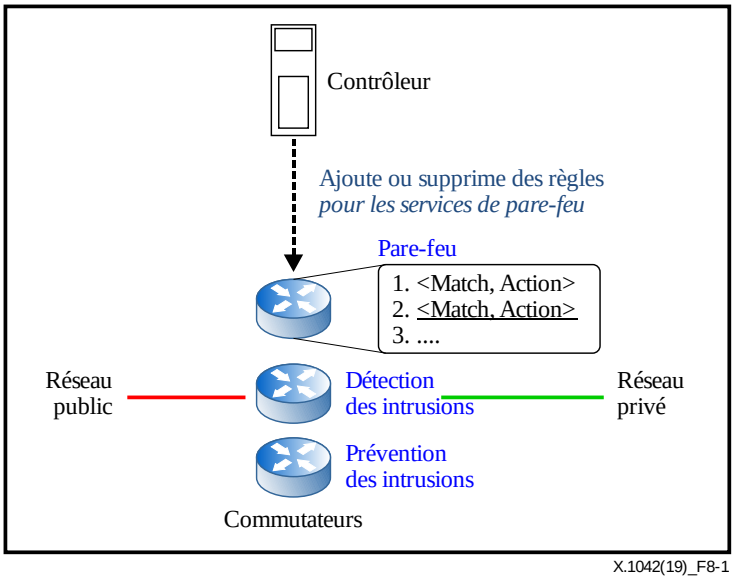


Figure 8-1 – Principe des services centralisés de pare-feu

8.1.2 Scénario de service d'un service centralisé de pare-feu

La Figure 8-2 montre un exemple de scénario d'un service centralisé de pare-feu visant à enrayer la propagation d'un ver.

Une condition préalable pour ce scénario est l'établissement par un gestionnaire de la sécurité d'une nouvelle politique pour l'application de pare-feu lorsque les informations relatives au ver sont identifiées. Afin d'empêcher la propagation de paquets contenant ce ver, l'utilisateur peut ajouter la nouvelle politique (par exemple, "abandonner les paquets contenant le fichier du ver") à l'application de pare-feu, qui s'exécute au-dessus du contrôleur SDN. Cela peut aussi faire l'objet d'une gestion centralisée, de telle sorte qu'un gestionnaire de la sécurité puisse établir des politiques de sécurité pour une application de pare-feu par l'intermédiaire d'un point unique, c'est-à-dire un contrôleur SDN.

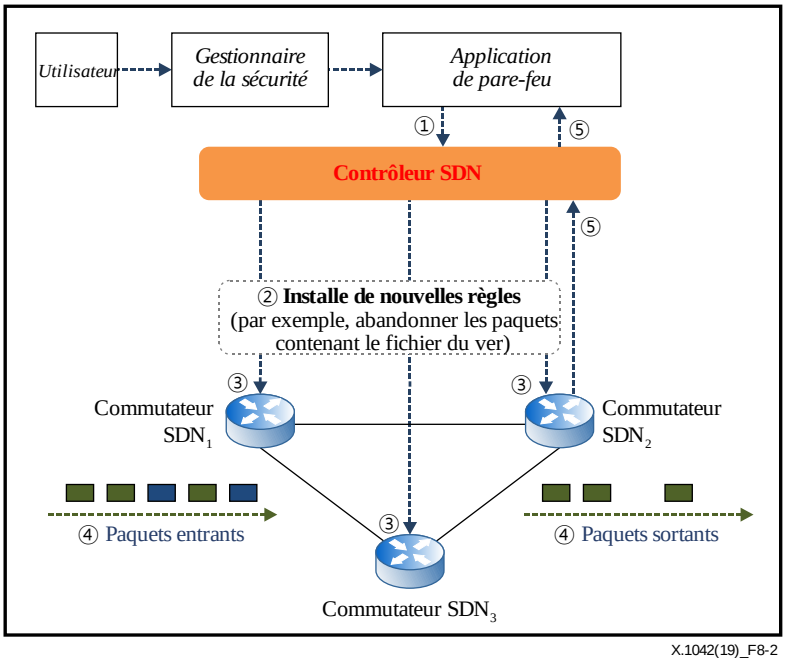


Figure 8-2 – Scénario intradomaine d'un service centralisé de pare-feu

– Etape 1. Une application de pare-feu installe de nouvelles règles.

  Une application de pare-feu doit établir une nouvelle règle lorsque des informations concernant un nouveau ver sont communiquées. La nouvelle règle (par exemple, "abandonner les paquets contenant le fichier du ver") est ajoutée au contrôleur SDN.

– Etape 2. Le contrôleur SDN distribue une nouvelle entrée de flux à tous les commutateurs SDN.

  Après avoir été installée, une nouvelle entrée de flux peut être distribuée à chaque commutateur par un contrôleur SDN. Par conséquent, le contrôleur SDN envoie une opération d'insertion de flux contenant la règle (par exemple, "abandonner les paquets contenant le fichier du ver") à tous les commutateurs SDN.

  Le nouveau ver signalé décrit dans le présent paragraphe peut être un ver déjà connu ou bien un ver encore inconnu. Dans le cas d'un ver connu, des mécanismes, par exemple des "signatures" ou des "empreintes" sont mis en place dans un service de pare-feu afin de détecter la menace et de s'en prémunir. Toutefois, un ver encore inconnu devrait faire l'objet d'une analyse et d'une détection avant que des mesures soient prises pour se protéger contre la menace qu'il représente. Les vers acheminent des données utiles malveillantes pouvant exploiter des applications ou services vulnérables. Ces vers peuvent être détectés au moyen de l'inspection des données utiles des paquets. L'Appendice II montre un exemple de détection par analyse des données par paquets.

– Etape 3. Tous les commutateurs SDN insèrent la nouvelle entrée de flux dans leur tableau de flux.

  Un commutateur SDN ajoute une entrée de flux relative à l'abandon des futurs paquets contenant le fichier du ver à son tableau de flux lorsqu'il reçoit l'opération d'insertion de flux concernant ce fichier. Le commutateur SDN peut abandonner les paquets qui contiennent le fichier du ver.

– Etape 4. Le commutateur SDN exécute ensuite les entrées de flux afin d'abandonner les paquets contenant des fichiers de ver.

  Un commutateur SDN abandonne complètement les paquets contenant un fichier de ver qu'il reçoit. En vertu des règles appliquées, aucun paquet contenant un fichier de ver ne pourra être remis.

– Etape 5. Un commutateur SDN signale à un contrôleur la réception d'un paquet inhabituel.

  Lorsqu'un commutateur SDN reçoit un paquet d'un type qu'il n'a jamais traité auparavant, il supprime le paquet en question et envoie un rapport au contrôleur au sujet de ce type de paquets. Le contrôleur détermine s'il s'agit d'une attaque. Si c'est le cas, il envoie un message à l'application de pare-feu et l'étape 1 est effectuée. Dans le cas contraire, le contrôleur conserve une entrée de flux ordinaire indiquant aux commutateurs comment traiter cette séquence pour les paquets suivants.

8.1.3 Scénario de service d'un service collaboratif de pare-feu

La Figure 8-3 montre un exemple de scénario d'une application de pare-feu fonctionnant en collaboration avec une application d'inspection approfondie des paquets (DPI) permettant d'assurer de manière centralisée la surveillance et la gestion des flux de téléphonie au moyen du protocole Internet (VoIP)/de téléphonie utilisant la technologie LTE (VoLTE). Ce scénario montre que l'application DPI commande chaque commutateur SDN pour la gestion des flux d'appel VoIP/VoLTE en manipulant des règles pouvant être ajoutées, supprimées ou modifiées de façon dynamique. Cette application peut coopérer avec une application de pare-feu pour assurer la protection du service VoIP/VoLTE. Plus précisément, un commutateur ayant une fonction de pare-feu réalise des vérifications de sécurité de base sur des paquets du flux inconnus. S'il découvre que le paquet en question est un paquet de flux d'appel VoIP inconnu qui contient des formes suspectes, il déclenche

le contrôleur SDN pour que ce dernier réalise une analyse de sécurité plus poussée du paquet d'appel VoIP suspect.

Une condition préalable pour ce scénario est l'établissement par un gestionnaire de la sécurité d'une nouvelle politique pour l'application de pare-feu et l'application DPI lorsque les informations relatives à une forme suspecte sont identifiées. Afin d'empêcher la présence de ces formes dans les paquets acheminés, l'utilisateur ajoute la nouvelle politique (par exemple, "abandonner les paquets contenant des formes suspectes") à l'application de pare-feu ainsi qu'à l'application DPI, qui s'exécutent au-dessus du contrôleur SDN. Cela peut aussi faire l'objet d'une gestion centralisée, de telle sorte qu'un gestionnaire de la sécurité puisse établir des politiques de sécurité pour des applications par l'intermédiaire d'un point unique, c'est-à-dire un contrôleur SDN.

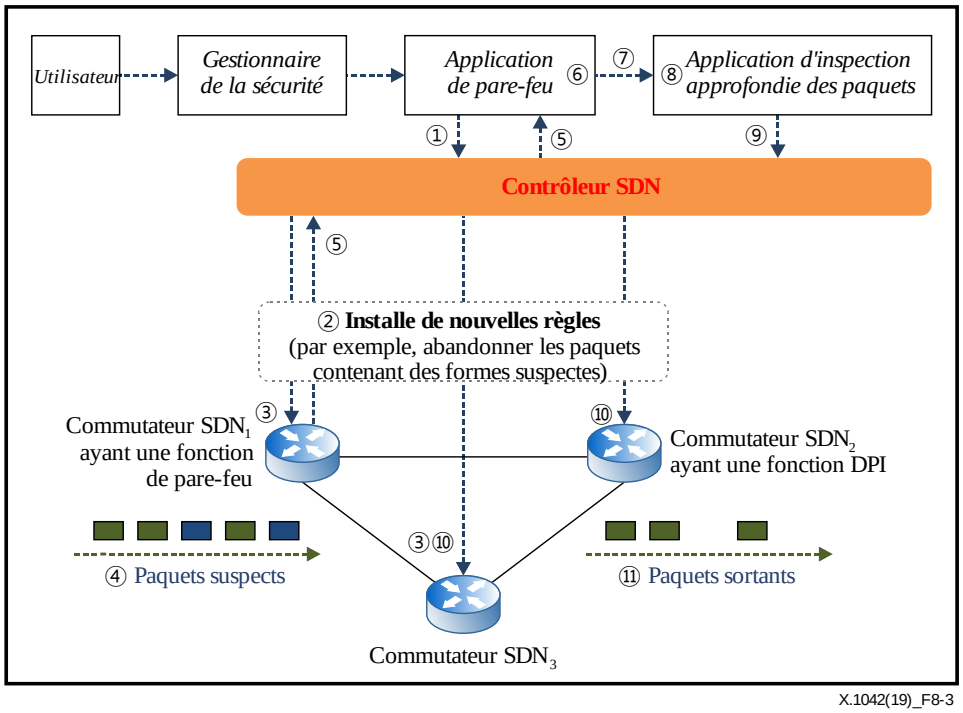


Figure 8-3 – Scénario intradomaine d'un service collaboratif de pare-feu

– Etape 1. L'application de pare-feu et l'application DPI installent de nouvelles règles concernant les formes connues.

  L'application de pare-feu et l'application DPI doivent établir une nouvelle règle lorsque des informations concernant une nouvelle forme sont communiquées. La nouvelle règle (par exemple, remettre les paquets contenant la forme en question au contrôleur SDN) est ajoutée au contrôleur SDN.

– Etape 2. Le contrôleur SDN distribue une nouvelle entrée de flux à tous les commutateurs SDN.

  Une nouvelle entrée de flux peut être distribuée à chaque commutateur par un contrôleur SDN. Par conséquent, le contrôleur SDN envoie une opération d'insertion de flux contenant la règle (par exemple, remettre les paquets contenant la forme en question) à tous les commutateurs SDN. Si chaque commutateur assure une fonction différente, le contrôleur SDN envoie à chacun d'eux des entrées de flux différentes. En d'autres termes, les commutateurs ayant une fonction de pare-feu ne doivent pas recevoir les entrées de flux relatives à l'inspection DPI.

– Etape 3. Tous les commutateurs SDN insèrent la nouvelle entrée de flux dans leurs tableaux de flux.

Un commutateur SDN ajoute une entrée de flux relative à l'acheminement des futurs paquets contenant la forme suspecte à son tableau de flux lorsqu'il reçoit l'opération d'insertion de flux du contrôleur SDN.

– Etape 4. Le commutateur SDN exécute les entrées de flux afin de remettre les paquets contenant des formes suspectes.

  Un commutateur SDN remet au contrôleur SDN les paquets contenant une forme suspecte qu'il reçoit. En vertu des règles appliquées, tous les paquets contenant des formes suspectes doivent être transférés au contrôleur SDN.

– Etape 5. Le commutateur SDN et le contrôleur SDN transmettent à l'application de pare-feu les éventuels paquets inhabituels qu'ils reçoivent.

  Lorsqu'un contrôleur SDN reçoit un paquet d'un type qu'il n'a jamais traité auparavant, il transmet ce paquet à l'application de pare-feu en vue d'une inspection de sécurité de base.

– Etape 6. L'application de pare-feu analyse le paquet inhabituel.

  L'application de pare-feu analyse les champs d'en-tête du paquet et détermine s'il s'agit d'un paquet contenant un signal de flux d'appel VoIP inconnu – par exemple, un paquet de protocole d'ouverture de session (SIP) – qui présente une forme suspecte.

– Etape 7. L'application de pare-feu déclenche l'application DPI.

  L'application de pare-feu déclenche une application appropriée, par exemple une application DPI, en vue d'une analyse de sécurité détaillée des paquets de signal suspects. Puis, elle transmet ces paquets à l'application DPI.

– Etape 8. L'application DPI analyse le paquet inhabituel.

  L'application DPI analyse les en-têtes et le contenu du paquet de signal, par exemple le numéro appelant et les en-têtes de description de session. Si, par exemple, l'application DPI considère le paquet comme détourné par des pirates informatiques ou comme un paquet recherchant des dispositifs VoIP/VoLTE, elle l'abandonne.

– Etape 9. L'application DPI demande au contrôleur SDN de bloquer le paquet en question.

  L'application DPI demande au contrôleur SDN de bloquer le paquet en question ainsi que les paquets suivants présentant le même identificateur d'appel.

– Etape 10. Le contrôleur SDN installe les nouvelles règles.

  Le contrôleur SDN distribue une nouvelle entrée de flux (par exemple, "abandonner les paquets") à tous les commutateurs SDN, comme dans l'étape 2. Par la suite, tous les paquets illicites seront abandonnés par ces commutateurs.

8.2 Service centralisé de leurre

8.2.1 Principe de base d'un service centralisé de leurre

On trouvera dans le présent paragraphe la description du principe de base d'un service centralisé de leurre. Le service de leurre peut gérer de manière dynamique les emplacements des leurres. Comme l'indique la Figure 8-4, un service centralisé de leurre gère des commutateurs et des nouveaux trajets de routage afin d'attirer les auteurs d'attaques vers un emplacement faisant office de piège: un leurre. Le leurre est configuré pour être la cible prévue des attaques et transmet les informations recueillies au service centralisé de leurre.

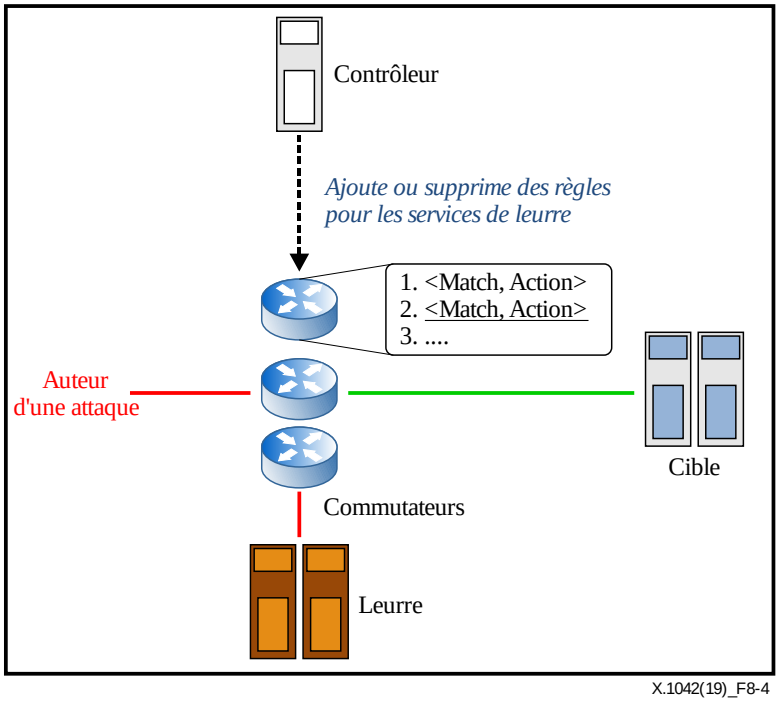


Figure 8-4 – Principe d'un service centralisé de leurre

8.2.2 Scénario de service d'un leurre centralisé

La Figure 8-5 montre un exemple de scénario d'un service centralisé de leurre consistant à ajouter aux commutateurs SDN un trajet de routage vers un leurre plutôt que vers la cible réelle.

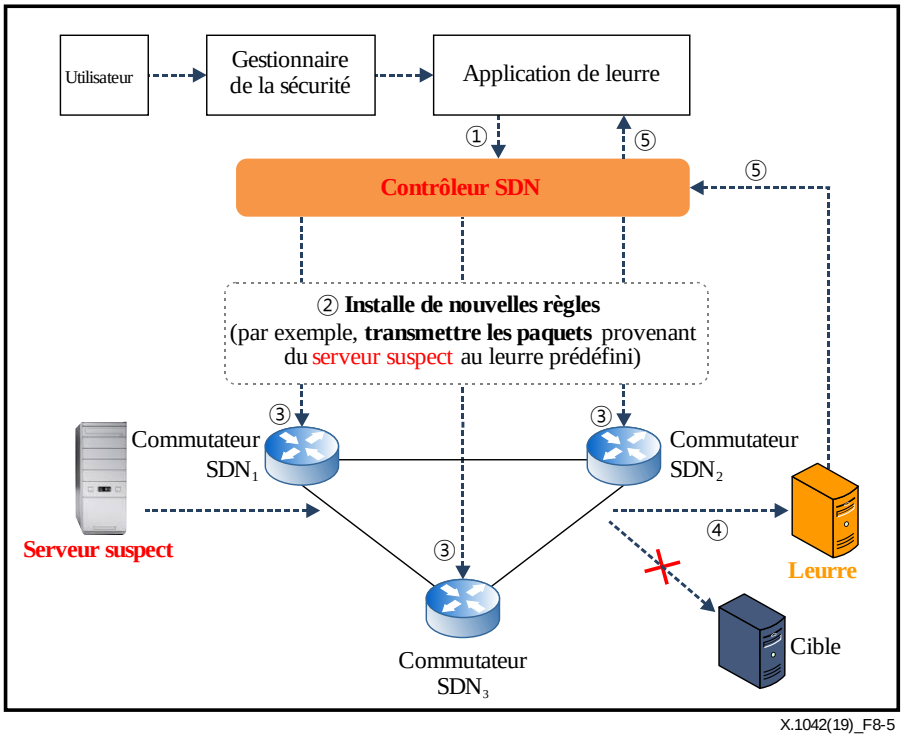


Figure 8-5 – Scénario intradomaine pour un service centralisé de leurre

– Etape 1. Une application de leurre installe de nouvelles règles au niveau du contrôleur SDN.

  Une application de leurre doit établir une nouvelle règle lorsque des informations concernant un serveur suspect sont communiquées. Afin de surveiller le trafic provenant d'un serveur suspect, la nouvelle règle (par exemple, "transmettre les paquets provenant du serveur suspect à un leurre") est ajoutée au contrôleur SDN par l'application de leurre, qui s'exécute au-dessus du contrôleur SDN.

– Etape 2. Un contrôleur SDN distribue les nouvelles règles aux commutateurs SDN appropriés.

  Après avoir été installée, une nouvelle règle peut être distribuée à chaque commutateur par un contrôleur SDN. Par conséquent, le contrôleur SDN envoie une opération d'insertion de flux contenant la règle (par exemple, "transmettre les paquets provenant du serveur suspect à un leurre") à tous les commutateurs SDN. Cela peut aussi faire l'objet d'une gestion centralisée, de telle sorte qu'un gestionnaire de la sécurité puisse établir des politiques de sécurité pour leur service par l'intermédiaire d'un point unique, c'est-à-dire un contrôleur SDN.

– Etape 3. Tous les commutateurs SDN insèrent les nouvelles règles dans leurs tableaux de flux.

  Suite à la réception de l'opération d'insertion de flux concernant le serveur suspect, tous les commutateurs SDN ajoutent à leur tableau de flux une entrée de flux relative à la transmission des futurs paquets provenant du serveur suspect à un leurre. Le commutateur SDN peut ensuite transmettre les paquets provenant du serveur suspect à un leurre.

– Etape 4. Un commutateur SDN exécute les nouvelles règles pour assurer le fonctionnement du service de leurre.

  Un commutateur SDN peut transmettre les paquets qu'il reçoit en provenance du serveur suspect à un leurre. En vertu des règles appliquées, aucun paquet provenant du serveur suspect ne pourra être remis à un serveur constituant une cible réelle. Les paquets ainsi acheminés sont réceptionnés dans le leurre.

– Etape 5. Le service de leurre communique un rapport portant sur les paquets suspects au contrôleur.

  Lorsqu'un service de leurre reçoit des paquets provenant de serveurs suspects, il traite ces paquets et envoie un rapport portant sur ce type de paquets au contrôleur, afin de permettre à ce dernier d'effectuer l'analyse de ces paquets.

8.3 Service centralisé d'atténuation des effets des attaques DDoS

8.3.1 Principe de base d'un service centralisé d'atténuation des effets des attaques DDoS

La Figure 8-6 illustre un service centralisé d'atténuation des effets des attaques DDoS. Ce service ajoute, supprime ou modifie des règles pour chaque commutateur SDN. Contrairement au "service centralisé de pare-feu" présentant un fonctionnement intradomaine, le service abordé dans ce paragraphe est principalement axé sur un fonctionnement interdomaines.

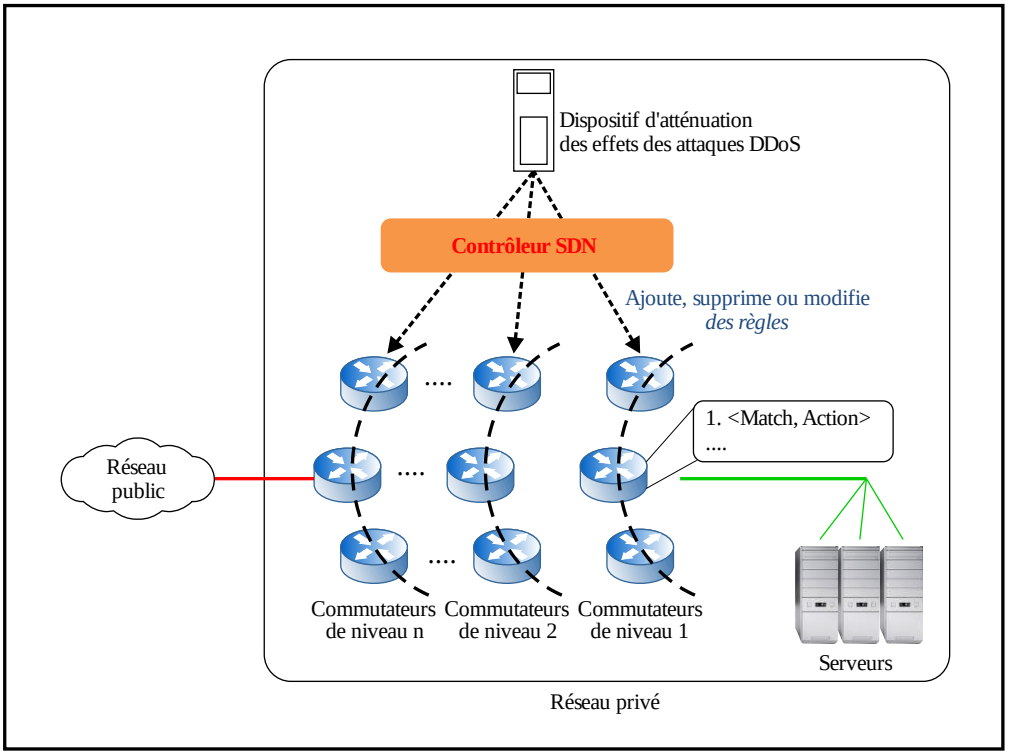


Figure 8-6 – Principe des services centralisés d'atténuation des effets des attaques DDoS

8.3.2 Service centralisé d'atténuation des effets des attaques DDoS pour des serveurs sans état

La Figure 8-7 montre un exemple de scénario d'un service centralisé d'atténuation des effets des attaques DDoS pour des serveurs d'un service de noms de domaine (DNS) sans état.

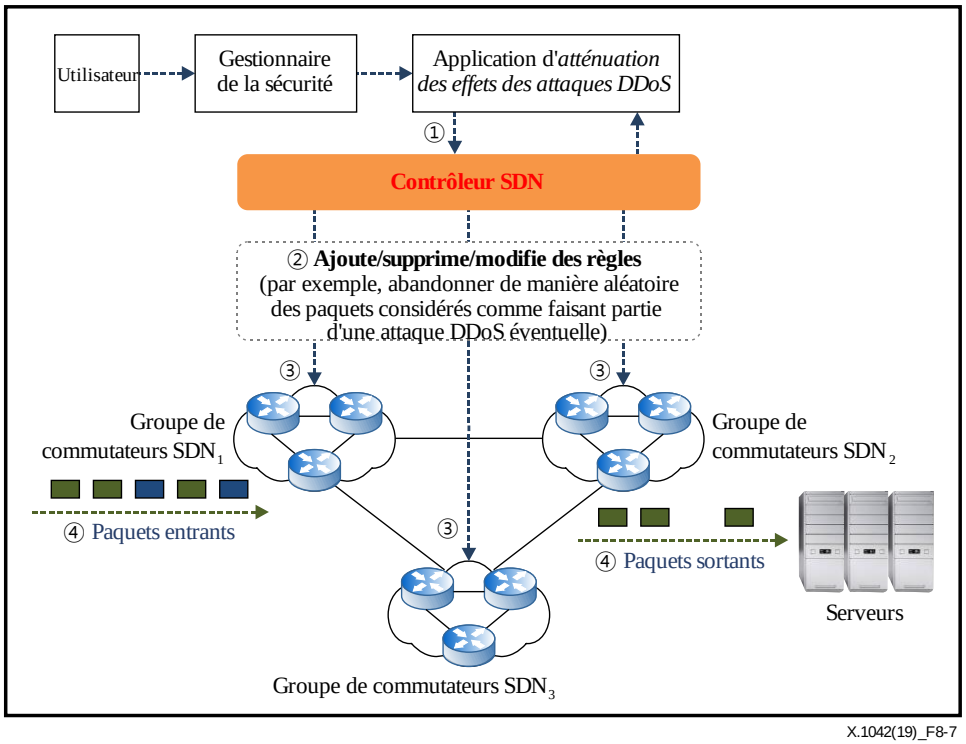


Figure 8-7 – Scénario interdomaines dans le cas d'un service centralisé d'atténuation des effets des attaques DDoS pour des serveurs sans état

– Etape 1. Une application d'atténuation installe de nouvelles règles pour le contrôleur SDN.

  Une application d'atténuation des effets des attaques DDoS doit établir une nouvelle règle lorsqu'une nouvelle attaque DDoS est signalée par le gestionnaire SM. En vue d'empêcher les paquets d'atteindre les serveurs et de gaspiller les ressources de ces derniers, la nouvelle règle (par exemple, "abandonner les paquets relatifs à une attaque DDoS de manière aléatoire selon une certaine probabilité") est ajoutée au contrôleur SDN. Cet ajout de règle est réalisé par l'application d'atténuation des effets des attaques DDoS, qui s'exécute au-dessus du contrôleur SDN.

– Etape 2. Un contrôleur SDN distribue les nouvelles règles aux commutateurs appropriés.

  Après avoir été installée, une nouvelle règle peut être distribuée à chaque commutateur par un contrôleur SDN. Par conséquent, le contrôleur SDN envoie une opération d'insertion de flux contenant la règle (par exemple, "abandonner de manière aléatoire les paquets considérés comme faisant partie d'une attaque DDoS selon une certaine probabilité") à tous les commutateurs SDN. Cela peut aussi faire l'objet d'une gestion centralisée, de telle sorte qu'un gestionnaire SM puisse établir des politiques de sécurité pour son service par l'intermédiaire d'un point unique, c'est-à-dire un contrôleur SDN.

– Etape 3. Tous les commutateurs SDN insèrent les nouvelles règles dans leurs tableaux de flux.

  Suite à la réception de l'opération d'insertion de flux concernant l'atténuation des effets d'une attaque DDoS, tous les commutateurs SDN ajoutent à leurs tableaux de flux une entrée de flux relative à l'abandon des futurs paquets considérés comme faisant partie de l'attaque DDoS. Par la suite, parmi les commutateurs du domaine, un commutateur SDN peut abandonner les paquets relatifs à l'attaque DDoS avec une probabilité proportionnelle à la gravité de cette attaque.

– Etape 4. Un commutateur SDN exécute les nouvelles règles pour atténuer les effets de l'attaque DDoS.

  Un commutateur SDN abandonne complètement les paquets de manière sélective lorsqu'il reçoit des paquets faisant partie d'une attaque DDoS. Les paquets relatifs à l'attaque DDoS sont abandonnés de façon aléatoire par les commutateurs SDN de chaque domaine, suivant les capacités de traitement et les caractéristiques des différents domaines. Par la suite, les résultats de ces abandons devront être communiqués au contrôleur SDN.

8.3.3 Service centralisé d'atténuation des effets des attaques DDoS pour des serveurs à états

La Figure 8-8 montre un exemple de scénario d'un procédé centralisé d'atténuation des effets des attaques DDoS pour des serveurs à états.

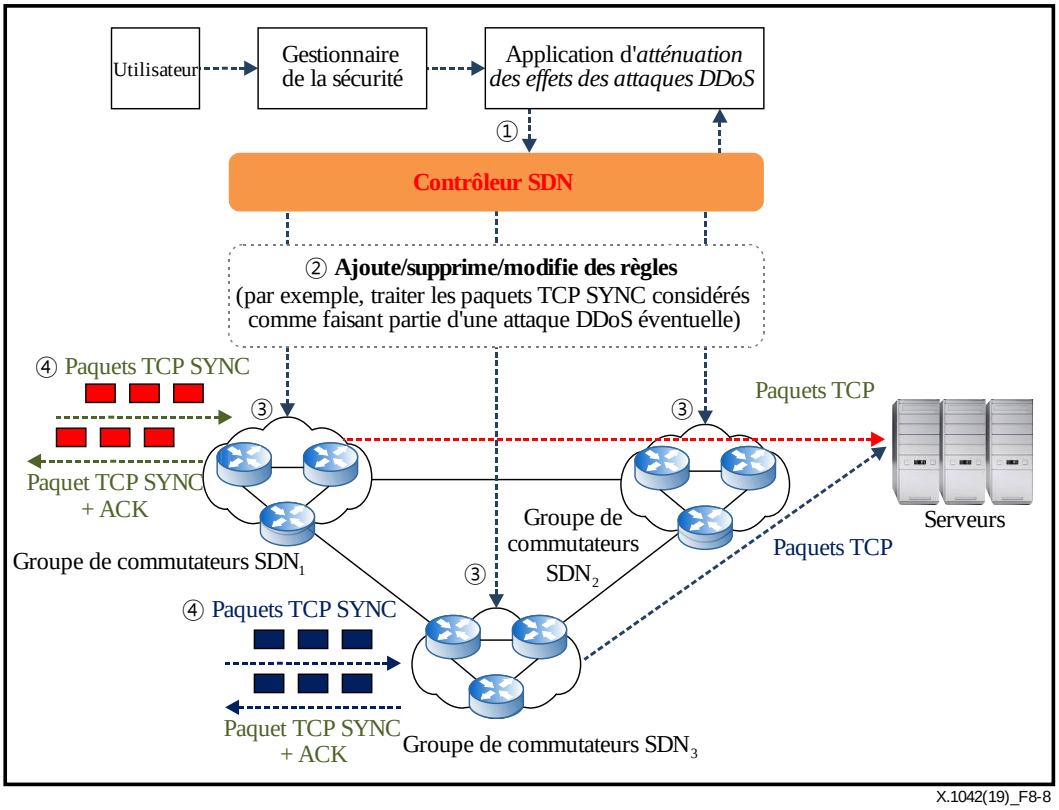


Figure 8-8 – Scénario interdomaines d'atténuation centralisée des effets des attaques DDoS pour des serveurs à états

– Etape 1. Une application d'atténuation installe de nouvelles règles pour le contrôleur SDN.

Une application d'atténuation des effets des attaques DDoS doit choisir quel commutateur tient le rôle de proxy pour le service TCP. L'ajout d'une nouvelle règle est réalisé par l'application d'atténuation des effets des attaques DDoS, qui s'exécute au-dessus du contrôleur SDN.

– Etape 2. Un contrôleur SDN distribue les nouvelles règles aux commutateurs appropriés.

Après avoir été installée, une nouvelle règle peut être distribuée aux commutateurs appropriés par un contrôleur SDN en vue de l'atténuation des effets des attaques DDoS. Par conséquent, le contrôleur SDN envoie une opération d'insertion de flux contenant la règle (par exemple, "générer les paquets TCP SYNC+ACK pour les paquets considérés comme faisant partie d'une attaque DDoS") à tous les commutateurs SDN. Par conséquent, une nouvelle règle est installée dans le commutateur choisi de sorte qu'il puisse générer sur demande les paquets TCP SYNC-ACK pour les paquets TCP SYNC. Si les mêmes demandes surviennent beaucoup plus fréquemment que prévu, le contrôleur SDN choisit un nouveau commutateur de sorte que ce commutateur se comporte comme un serveur. Pour les paquets TCP SYNC normaux, le commutateur transfère la session TCP au serveur correspondant dans le réseau privé. Cela peut aussi faire l'objet d'une gestion centralisée, de telle sorte qu'un gestionnaire SM puisse établir des politiques de sécurité pour son service par l'intermédiaire d'un point unique, c'est-à-dire le contrôleur SDN.

– Etape 3. Tous les commutateurs SDN insèrent les nouvelles règles dans leur tableau de flux.

Suite à la réception de l'opération d'insertion de flux concernant les attaques DDoS, tous les commutateurs SDN ajoutent à leur tableau de flux une entrée de flux relative à l'abandon des futurs paquets considérés comme faisant partie de l'attaque DDoS. Par la suite, le commutateur SDN peut générer des paquets TCP SYNC-ACK avec une probabilité proportionnelle à la gravité de l'attaque DDoS.

– Etape 4. Un commutateur SDN exécute les nouvelles règles pour atténuer les effets de l'attaque DDoS.

  Un commutateur SDN répond entièrement aux paquets TCP SYNC provenant d'un serveur hostile de manière aléatoire lorsqu'il reçoit des paquets faisant partie d'une attaque DDoS. Les demandes s'inscrivant dans le cadre d'attaques DDoS adressées à des serveurs à états sont traitées par des commutateurs plutôt que par des serveurs réels. Par la suite, les résultats d'exécution du commutateur SDN relatifs à l'atténuation des effets de l'attaque DDoS doivent être transmis au contrôleur SDN.

8.4 Service centralisé de gestion des dispositifs illicites

8.4.1 Principe de base d'un service centralisé de gestion des dispositifs illicites

On trouvera dans le présent paragraphe la description du principe de base d'un service centralisé de gestion des dispositifs illicites. Comme le montre la Figure 8-9, un service centralisé de gestion des dispositifs illicites gère la liste noire répertoriant les dispositifs illicites afin de bloquer le trafic provenant de ces dispositifs. La liste des dispositifs illicites est stockée dans une base de données contenant la liste noire et peut être mise à jour de façon manuelle ou automatique par des applications indépendantes. Le gestionnaire centralisé des dispositifs illicites charge régulièrement la liste des dispositifs illicites depuis la base de données contenant la liste noire et signale ces cas à l'application de gestion des dispositifs illicites, qui génère de nouvelles règles de sécurité pour bloquer le trafic de réseau en provenance ou à destination de ces dispositifs illicites.

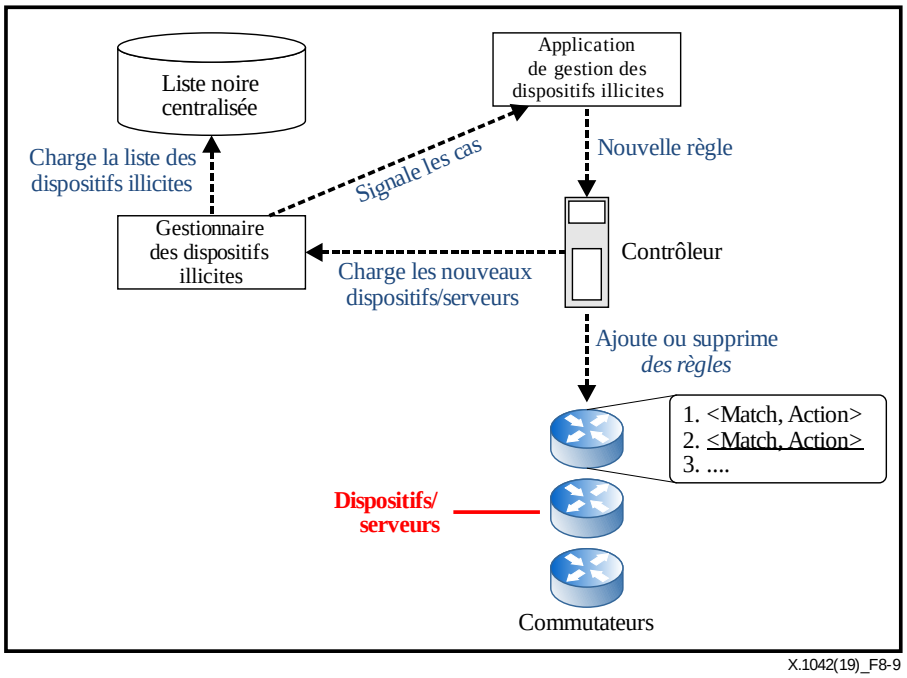


Figure 8-9 – Principe d'un service centralisé de gestion des dispositifs illicites

8.4.2 Scénario de service d'un service centralisé de gestion des dispositifs illicites

La Figure 8-10 montre un exemple de scénario d'un service centralisé de gestion des dispositifs illicites visant à bloquer le trafic provenant d'un dispositif mobile volé.

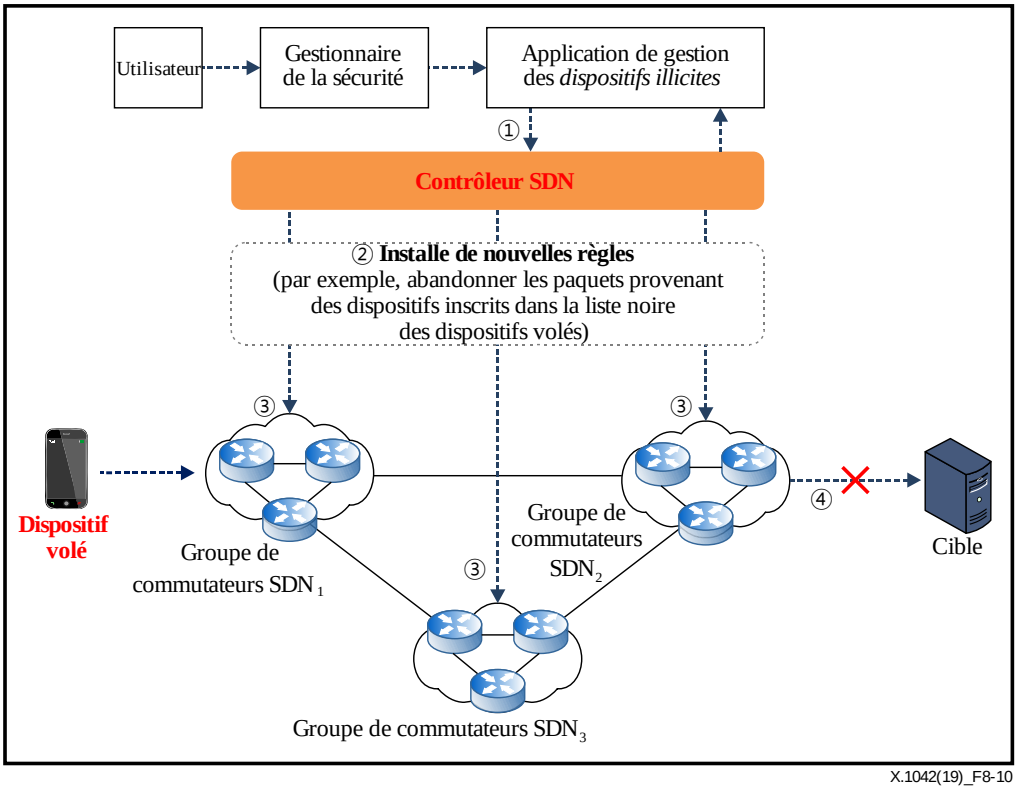


Figure 8-10 – Scénario interdomaines pour un service centralisé de gestion des dispositifs illicites

– Etape 1. Une application de gestion des dispositifs illicites installe de nouvelles règles.

  Une application de gestion des dispositifs illicites doit établir une nouvelle règle lorsque les informations concernant de nouveaux dispositifs volés sont communiquées par le gestionnaire centralisé des dispositifs illicites. Une condition préalable pour ce scénario est l'ajout par l'application de gestion des dispositifs illicites ou le gestionnaire de la sécurité de la nouvelle règle (par exemple, "abandonner les paquets provenant des dispositifs figurant dans la liste noire centralisée des dispositifs volés") au niveau du contrôleur SDN.

– Etape 2. Un contrôleur SDN distribue les nouvelles règles.

  Après avoir été installée, une nouvelle règle peut être distribuée à chaque commutateur par un contrôleur SDN. Par conséquent, le contrôleur SDN envoie une opération d'insertion de flux contenant la règle (par exemple, "abandonner les paquets provenant des nouveaux dispositifs volés") à tous les commutateurs SDN. Cela peut aussi faire l'objet d'une gestion centralisée, de telle sorte qu'un gestionnaire centralisé des dispositifs illicites ou un gestionnaire SM puisse établir des politiques de sécurité pour son service par l'intermédiaire d'un point unique, c'est-à-dire un contrôleur SDN.

– Etape 3. Tous les commutateurs SDN insèrent les nouvelles règles dans leurs tableaux de flux.

  Suite à la réception de l'opération d'insertion de flux concernant les dispositifs volés, tous les commutateurs SDN ajoutent à leur tableau de flux une entrée de flux relative à l'abandon des futurs paquets provenant de ces dispositifs.

– Etape 4. Un commutateur SDN exécute les nouvelles règles.

  Un commutateur SDN abandonne complètement les paquets qu'il reçoit en provenance de ces dispositifs. En vertu des règles appliquées, aucun paquet provenant de ces dispositifs ne pourra être remis. Par la suite, les résultats d'exécution doivent être transmis au contrôleur SDN.

NOTE – Il est important que les dispositifs illicites soient identifiés. Une identité unique, attribuée par le gestionnaire centralisé des dispositifs illicites, est utilisée pour identifier un dispositif illicite. Si le contrôleur SDN n'identifie que l'adresse réseau, comme l'adresse du protocole Internet (IP) d'un dispositif et l'adresse de la commande d'accès au support (MAC) qui peuvent être modifiées de façon dynamique, une nouvelle règle est installée et l'ancienne règle est supprimée au niveau du contrôleur SDN, chaque fois que l'adresse réseau d'un dispositif illicite est modifiée.

8.5 Service de gestion du contrôle d'accès

8.5.1 Principe de base d'un service de gestion du contrôle d'accès

On trouvera dans le présent paragraphe la description du principe de base d'un service de gestion du contrôle d'accès (ACM). Le module ACM et un contrôleur SDN peuvent gérer les politiques de droit d'accès de façon hiérarchique. Comme le montre la Figure 8-11, un module ACM gère les droits d'accès afin d'empêcher l'accès illégal aux ressources.

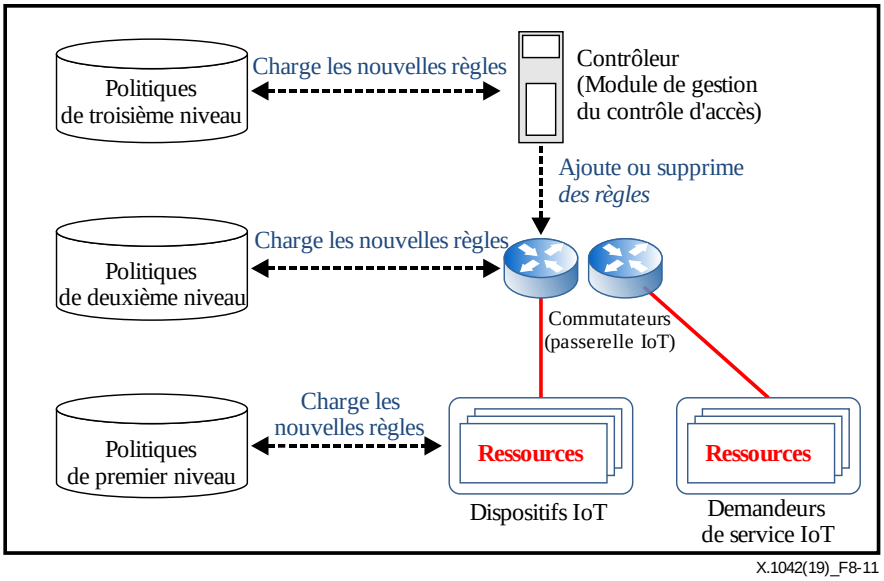


Figure 8-11 – Principe d'un service de gestion du contrôle d'accès

8.5.2 Scénario de service d'un service de gestion du contrôle d'accès

La Figure 8-12 montre un exemple de scénario d'un service ACM géré par un contrôleur de la sécurité. Ce scénario fait intervenir à la fois un contrôleur et des commutateurs SDN.

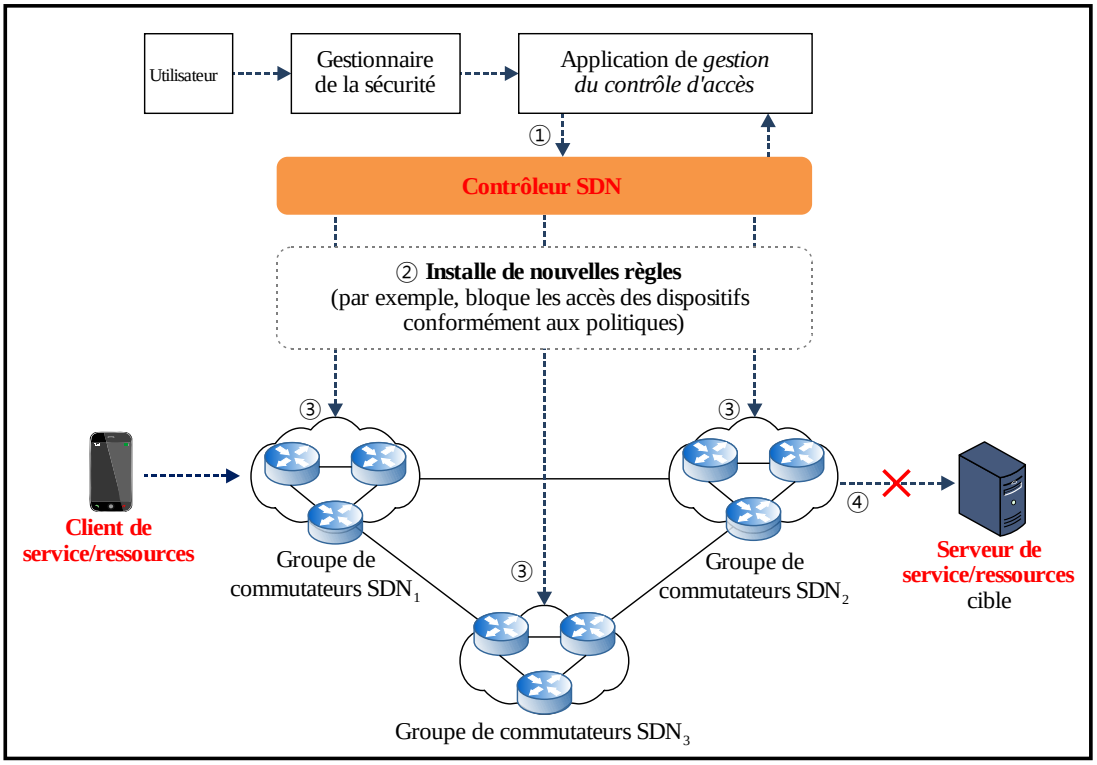


Figure 8-12 – Scénario interdomaines pour un service de gestion du contrôle d'accès

– Etape 1. Une application ACM installe de nouvelles politiques provenant du gestionnaire SM.

  Une application ACM doit établir de nouvelles politiques relatives à l'accès aux ressources pour des dispositifs de service/ressources répartis (par exemple, des dispositifs IoT). Une condition préalable pour ce scénario est l'ajout par le gestionnaire de la sécurité de nouvelles politiques à cette application ACM.

– Etape 2. Un contrôleur SDN distribue les nouvelles règles.

  Une ou plusieurs nouvelles règles doivent être stockées. Elles doivent ensuite être distribuées à chaque commutateur par un contrôleur SDN. Le contrôleur SDN peut envoyer une demande d'accès en vue d'exploiter la ou les ressources à un dispositif de service/ressources. Dans ce cas, un contrôleur SDN ne reçoit aucune demande des commutateurs SDN relative à la distribution des règles. Les commutateurs SDN peuvent être en mesure de demander au contrôleur SDN de fournir des règles d'accès pour des ressources de dispositifs de service/ressources avant de lui envoyer des demandes relatives à la distribution de règles.

– Etape 3. Tous les commutateurs SDN ajoutent les nouvelles règles dans leur base de données locale.

  Tous les commutateurs SDN ajoutent les nouvelles règles dans leur base de données locale afin de traiter les demandes d'autorisation d'accès aux dispositifs de service/ressources.

– Etape 4. Un commutateur SDN exécute les nouvelles règles.

  Un commutateur SDN peut complètement abandonner les paquets qu'il reçoit en provenance d'un client de service/ressources, conformément aux règles d'accès. Dans le cas considéré, chaque domaine de commutateur SDN doit pouvoir avoir plusieurs règles d'accès différentes, en fonction des capacités de chacun de ces domaines. En vertu des règles appliquées, aucun paquet provenant de ces clients ne pourra être remis par un commutateur SDN. Tout paquet ne faisant l'objet d'aucune règle d'accès doit être signalé au contrôleur SDN en vue de sa gestion par l'application ACM.

Appendice I

Critères applicables aux services de sécurité fondés sur les réseaux SDN

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

Le présent appendice fournit des critères applicables à différents services de sécurité.

I.1 Critères applicables aux services de sécurité dans des réseaux intradomaine

I.1.1 Service centralisé de pare-feu

Les anciens pare-feu présentent des problèmes, par exemple en ce qui concerne leur coût important, leur qualité de fonctionnement, la gestion du contrôle d'accès, l'établissement de politiques et les mécanismes d'accès en mode paquets. Afin de remédier à ces problèmes, la présente Recommandation décrit le cadre d'un service centralisé de pare-feu fondé sur les réseaux SDN. Les règles de pare-feu peuvent être gérées de façon flexible par un serveur centralisé. Les protocoles SDN existants peuvent être utilisés par l'intermédiaire d'interfaces normalisées entre les applications de pare-feu et les commutateurs.

– Coût

  Le coût relatif à l'ajout de pare-feu aux ressources de réseau, par exemple les routeurs, les passerelles et les commutateurs, est considérable car les pare-feu doivent être ajoutés à chaque ressource de réseau. Afin de résoudre ce problème, chaque ressource de réseau peut être gérée de façon centralisée, afin qu'un seul pare-feu soit manipulé par un serveur centralisé.

– Qualité de fonctionnement

  La qualité de fonctionnement des pare-feu est souvent inférieure au débit de liaison de leurs interfaces de réseau. Chaque ressource de réseau doit vérifier les règles de pare-feu indépendamment de l'état du réseau. Dans le cadre présenté, les pare-feu peuvent être déployés de façon adaptative en fonction de l'état du réseau.

– Gestion du contrôle d'accès

  Etant donné qu'il peut y avoir des centaines de ressources de réseau au sein d'un réseau administré, la gestion dynamique du contrôle d'accès pour les services de sécurité tels que les pare-feu se révèle problématique. Cela provient du fait que des règles de pare-feu doivent être ajoutées de façon dynamique pour les nouvelles attaques de réseau.

– Etablissement de politiques

  Une politique doit être établie pour chaque ressource de réseau. Toutefois, il est difficile de décrire quels types de flux sont autorisés et refusés dans le réseau considéré d'une organisation particulière. Par conséquent, une vision centralisée peut être utile afin de déterminer des politiques de sécurité pour un réseau de ce type.

– Mécanisme d'accès en mode paquets

  En pratique, un mécanisme d'accès en mode paquets n'est pas suffisant, étant donné que l'unité de base du contrôle d'accès est généralement un utilisateur ou une application. Par conséquent, il est nécessaire qu'un administrateur définisse et ajoute au service de pare-feu des règles à l'échelle de l'application.

I.1.2 Service centralisé de leurre

Les anciens leurres présentent des problèmes, par exemple en ce qui concerne leur coût important, leur qualité de fonctionnement, la gestion du contrôle d'accès, l'établissement de politiques et les mécanismes d'accès en mode paquets. Afin de remédier à ces problèmes, la présente

Recommandation décrit le cadre d'un service centralisé de leurre fondé sur les réseaux SDN. Les emplacements des leurres peuvent être gérés de façon flexible par un serveur centralisé. Les protocoles SDN existants peuvent être utilisés par l'intermédiaire d'interfaces normalisées entre les applications de leurre et les commutateurs.

– Coût

  Le coût relatif à la mise en oeuvre de leurres supplémentaires dans un réseau est considérable en raison de la nécessité d'employer des ressources de réseau supplémentaires, par exemple des serveurs pour accueillir les leurres. Afin de résoudre ce problème, les emplacements des leurres peuvent être gérés de façon flexible par un serveur centralisé.

– Qualité de fonctionnement

  La qualité de fonctionnement des leurres dépend de la capacité des serveurs. Chaque leurre fonctionne toujours de la même manière, indépendamment de l'état du réseau ou des circonstances de l'attaque. Dans le cadre présenté, les leurres peuvent être déployés de façon adaptative en fonction de l'état du réseau ou des circonstances de l'attaque.

– Gestion du contrôle d'accès

  Etant donné qu'il peut y avoir des centaines de ressources de réseau au sein d'un réseau administré, la configuration dynamique des leurres se révèle problématique. Cela provient du fait que les emplacements des leurres doivent être modifiés de façon dynamique pour faire face à de nouvelles attaques.

– Etablissement de politiques

  Une politique doit être établie pour chaque ressource de réseau. Toutefois, il est difficile de déterminer des emplacements de leurre particuliers pour faire face à des attaques suspectes en fonction de l'état du réseau et des circonstances de l'attaque. Par conséquent, une vision centralisée peut être utile afin d'ajuster les politiques de sécurité dans le temps.

– Mécanisme de déploiement de leurres

  Les emplacements des leurres doivent être déterminés de façon appropriée en fonction de l'état du réseau et des circonstances de l'attaque. Un service centralisé de leurre fondé sur les réseaux SDN détermine l'emplacement optimal pour assurer la surveillance des attaques et y répondre en temps réel. Le leurre est configuré de manière centralisée par un serveur centralisé pour être la cible des attaques.

I.2 Critères applicables aux services de sécurité dans des réseaux interdomaines

I.2.1 Service centralisé d'atténuation des effets des attaques DDoS

Un service centralisé d'atténuation des effets des attaques DDoS protège les serveurs contre les attaques DDoS qui ne proviennent pas des réseaux privés, c'est-à-dire qui proviennent des réseaux publics. Les serveurs sont classés suivant s'ils sont "sans état" (par exemple, les serveurs DSN) ou "à états" (par exemple, les serveurs web). La Figure 8-6 illustre la configuration d'un service d'atténuation des effets des attaques DDoS dans un réseau privé. Les commutateurs du réseau privé sont configurés selon des niveaux de domaine hiérarchiques: commutateurs de niveau 1, commutateurs de niveau 2, etc., jusqu'aux commutateurs de niveau n, qui forment des lignes de défense dynamiques contre diverses attaques DDoS.

Les services centralisés d'atténuation des effets des attaques DDoS présentent des problèmes, par exemple en ce qui concerne leur coût important, leur qualité de fonctionnement, la gestion du contrôle d'accès, l'établissement de politiques et les mécanismes d'accès en mode paquets. Afin de remédier à ces problèmes, la présente Recommandation décrit le cadre d'un service centralisé d'atténuation des effets des attaques DDoS fondé sur les réseaux SDN. Les règles d'atténuation des effets des attaques DDoS peuvent être gérées de façon flexible par un serveur centralisé. Les protocoles SDN existants

peuvent être utilisés par l'intermédiaire d'interfaces normalisées entre les applications d'atténuation des effets des attaques DDoS et les commutateurs.

– Coût

  Chaque ressource de réseau peut être gérée de façon flexible et centralisée pour un coût minimal en faisant en sorte que les commutateurs soient configurés et manipulés par un serveur centralisé selon différents niveaux. Lorsque la gravité des attaques DDoS contre un serveur augmente, les commutateurs des différents niveaux abandonnent des paquets de façon sélective afin de réduire les effets des attaques en question. Autrement dit, les paquets suspects faisant partie d'une attaque DDoS seront abandonnés plus tôt sur le trajet de routage menant vers le serveur victime de l'attaque.

– Qualité de fonctionnement

  La qualité de fonctionnement d'un service centralisé d'atténuation des effets des attaques DDoS est souvent inférieure au débit de liaison de ses interfaces de réseau. Dans les anciens services, chaque ressource de réseau doit vérifier les règles d'atténuation des effets des attaques DDoS indépendamment de l'état du réseau. Toutefois, dans le cadre présenté, les applications d'atténuation des effets des attaques DDoS peuvent être déployées de façon adaptative en fonction de l'état du réseau.

– Gestion du contrôle d'accès

  Etant donné qu'il peut y avoir des centaines de ressources de réseau au sein d'un réseau administré, la gestion dynamique du contrôle d'accès pour les services de sécurité tels que l'atténuation des effets des attaques DDoS se révèle problématique. Cela provient du fait que des règles d'atténuation des effets des attaques DDoS doivent être ajoutées de façon dynamique pour les nouvelles attaques DDoS.

– Etablissement de politiques

  Une politique doit être établie pour chaque ressource de réseau. Toutefois, il est difficile de déterminer des politiques particulières relatives à l'abandon de paquets pour faire face à des attaques DDoS en fonction de l'état du réseau. Par conséquent, une vision centralisée peut être utile afin d'ajuster les politiques de sécurité dans le temps.

– Mécanisme de détection des attaques DDoS

  La détection des attaques DDoS est réalisée en analysant l'intervalle qui sépare les demandes de services d'un client. Le mécanisme de détection des attaques DDoS détermine la probabilité que des demandes provenant d'un client fassent partie d'une attaque DDoS et augmente la fréquence des abandons relatifs à ces demandes proportionnellement à la probabilité calculée.

I.2.2 Service centralisé de gestion des dispositifs illicites

Les anciens services de gestion des dispositifs illicites présentent des problèmes, par exemple en ce qui concerne leur coût important, leur qualité de fonctionnement, la gestion du contrôle d'accès, l'établissement de politiques et les mécanismes d'accès en mode paquets. Afin de remédier à ces problèmes, la présente Recommandation décrit le cadre d'un service centralisé de gestion des dispositifs illicites fondé sur les réseaux SDN. Les règles relatives à l'inscription de dispositifs dans une liste noire peuvent être gérées dans leur ensemble. Les protocoles SDN existants peuvent être utilisés par l'intermédiaire d'interfaces normalisées entre les applications de dispositifs illicites et les commutateurs.

– Coût

  Le coût relatif à la mise à jour des listes noires pour les ressources de réseau, par exemple les routeurs, les passerelles et les commutateurs est considérable en raison de la nécessité de mettre à jour les listes noires pour chaque ressource de réseau individuellement. Afin de résoudre ce problème, les règles de sécurité relatives aux listes noires pour chaque ressource

de réseau peuvent être gérées de façon centralisée, de façon qu'un seul service de gestion des dispositifs illicites soit manipulé par un serveur centralisé.

– Qualité de fonctionnement

  Etant donné que, contrairement aux anciens services de gestion, les paquets provenant de dispositifs figurant sur une liste noire sont abandonnés au début du trajet de routage, dans la pratique, la qualité de fonctionnement des services centralisés de gestion des dispositifs illicites peut être améliorée.

– Gestion du contrôle d'accès

  Lorsque les listes noires sont gérées de façon locale, il n'est pas facile de synchroniser les listes noires réparties au niveau local, étant donné qu'il peut y avoir des centaines de ressources de réseau situées dans différents pays. Les règles de sécurité doivent être ajoutées de façon dynamique pour les nouveaux dispositifs illicites.

– Etablissement de politiques

  Une politique doit être établie pour chaque ressource de réseau. Toutefois, il est difficile de décrire quels dispositifs ne sont pas autorisés dans le réseau considéré d'une organisation particulière. Par conséquent, une vision centralisée peut être utile afin de déterminer des politiques de sécurité pour un réseau de ce type.

– Mécanisme de mise à jour d'une liste noire

  Il est important de tenir à jour la liste noire répertoriant les dispositifs illicites. Par conséquent, les anciens services doivent régulièrement mettre à jour la base de données contenant la liste noire de façon à conserver les informations les plus récentes concernant les dispositifs illicites. Dans le cas d'un service centralisé de gestion des dispositifs illicites, la liste noire est gérée de façon centralisée par un serveur centralisé en tant que base de données logique unique.

I.2.3 Service de gestion du contrôle d'accès

Les services ACM présentent des problèmes, par exemple en ce qui concerne leur coût important, leur qualité de fonctionnement, la gestion du contrôle d'accès, l'établissement de politiques et les mécanismes d'accès en mode paquets. Afin de remédier à ces problèmes, la présente Recommandation décrit un service ACM fondé sur les réseaux SDN. Les règles relatives à l'inscription de dispositifs dans une liste blanche peuvent être gérées dans des services de réseaux répartis (par exemple un contrôleur SDN, un commutateur). Les protocoles SDN existants peuvent être utilisés par l'intermédiaire d'interfaces normalisées entre les applications ACM et les commutateurs au moyen d'un contrôleur SDN.

– Coût

  Le coût relatif à la mise à jour des listes blanches pour les ressources de réseau, par exemple les routeurs, les passerelles et les commutateurs, est considérable en raison de la nécessité de mettre à jour les listes blanches pour de nombreuses ressources de réseau. Afin de résoudre ce problème, les politiques de sécurité relatives aux listes blanches pour chaque ressource de réseau peuvent être gérées de façon centralisée, de façon qu'un seul service ACM soit manipulé par un serveur centralisé.

– Qualité de fonctionnement

  Etant donné que, contrairement aux anciens services de gestion, les paquets provenant des dispositifs qui ne disposent pas de droits d'accès sont abandonnés au début du trajet de routage, dans la pratique, la qualité de fonctionnement du service ACM peut être améliorée dans la pratique. En outre, les informations relatives aux droits d'accès seront subdivisées et stockées dans les ressources de réseau en fonction de leur niveau de sécurité

– Gestion du contrôle d'accès

  Lorsque les listes blanches sont gérées de façon locale, il n'est pas facile de les synchroniser, étant donné qu'il peut y avoir des centaines de ressources de réseau situées dans différents pays. Les règles de sécurité doivent être ajoutées de façon dynamique pour transmettre de nouveaux droits d'accès aux ressources de réseau.

– Etablissement de politiques

  Une politique doit être établie pour chaque ressource de réseau en fonction de son niveau de sécurité. Toutefois, il est difficile de décrire quels dispositifs IoT ne sont pas autorisés dans le réseau d'une organisation donnée dans le cadre d'un service ACM. Par conséquent, une vision centralisée peut être utile afin de déterminer des politiques de sécurité pour un réseau de ce type.

– Mécanisme de mise à jour d'une liste blanche

  Il est très important de tenir à jour une liste blanche des droits d'accès pour les dispositifs IoT. Par conséquent, les anciens services doivent régulièrement mettre à jour périodiquement la base de données contenant la liste blanche, de façon à conserver les informations les plus récentes concernant les droits d'accès éventuels pour les dispositifs IoT. Dans le cas d'un service ACM, la liste blanche est gérée de façon centralisée par un serveur centralisé en tant que base de données logique unique. En outre, certaines parties des politiques peuvent être réparties dans les ressources de réseau.

Appendice II

Exemple de détection par analyse des données par paquets

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

La détection par analyse des données par paquets doit être prise en charge afin de permettre la détection de certaines attaques telles que les fichiers de ver ainsi que l'atténuation de leurs effets. L'administrateur configure les politiques de façon à détecter de manière aléatoire seulement certains paquets du flux, et non la totalité de ces paquets, afin d'obtenir une meilleure qualité de fonctionnement. Un schéma possible pour la détection par analyse des données par paquets [b-ICIN SDNSec] consiste à analyser les m premiers paquets consécutifs de chaque flux. Ce schéma peut être paramétré pour s'appliquer à tous les flux ou seulement à ceux qui remplissent certaines conditions, par exemple les paquets provenant d'une certaine adresse IP ou qui se dirigent vers une destination déterminée.

Le protocole OpenFlow [b-ONF TS-012], en tant que mise en oeuvre d'une interface SDN descendante, peut être étendu de façon à prendre en charge la détection par analyse de données par paquets. Deux caractéristiques supplémentaires peuvent être ajoutées au format de l'entrée de flux. Ces modifications doivent être répercutées dans le contrôleur ainsi que dans les commutateurs. L'une de ces caractéristiques correspond au schéma qui comprend la détection par analyse de données par paquets. La seconde correspond à la description des flux qui remplissent les conditions configurées par l'administrateur ou par des applications. Une action facultative (OFPAT_DETECTION) doit ensuite être ajoutée au paragraphe 5.12 de [b-ONF TS-012], comme indiqué dans le texte suivant en italique: *Optional Action: the Detection action forwards a packet to a specified OpenFlow port then to security appliances (e.g., FW, IDP, DPI, etc.) for further data scan detection.* Cette nouvelle action est semblable à l'action OFPAT_OUTPUT du protocole OpenFlow. Enfin, les structures des actions doivent être mises à jour au paragraphe 7.2.4 de [b-ONF TS-012], comme indiqué par le texte ci-après en italique:

```
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);
```

Appendice III

Architecture de mise en oeuvre des services de sécurité fondés sur les réseaux SDN

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

III.1 Cadre de l'IETF pour l'interface avec la fonction de sécurité de réseau reposant sur des réseaux SDN

III.1.1 Aperçu général

Le présent paragraphe décrit le cadre de l'IETF pour l'interface avec la fonction de sécurité de réseau (I2NSF) reposant sur des réseaux SDN applicable aux services de sécurité fondés sur le nuage, par exemple les pare-feu ainsi que les fonctions DPI et d'atténuation des effets des attaques DDoS. Les réseaux SDN permettent la mise en place de règles de filtrage de certains paquets au niveau des commutateurs du réseau au moyen du contrôle de leurs règles relatives à l'acheminement des paquets. En exploitant cette capacité des réseaux SDN, il est possible d'optimiser le processus de mise en oeuvre des services de sécurité dans le cadre I2NSF.

La Figure III.1 illustre un cadre I2NSF [b-IETF RFC 8329] reposant sur des réseaux SDN pour assurer les services de sécurité à l'échelle du réseau. Dans ce cadre, la mise en oeuvre des règles de politique de sécurité est partagée entre les commutateurs SDN et les fonctions de sécurité de réseau (NSF). Dans ce qui suit, on utilisera le protocole NETCONF et le langage de modélisation YANG.

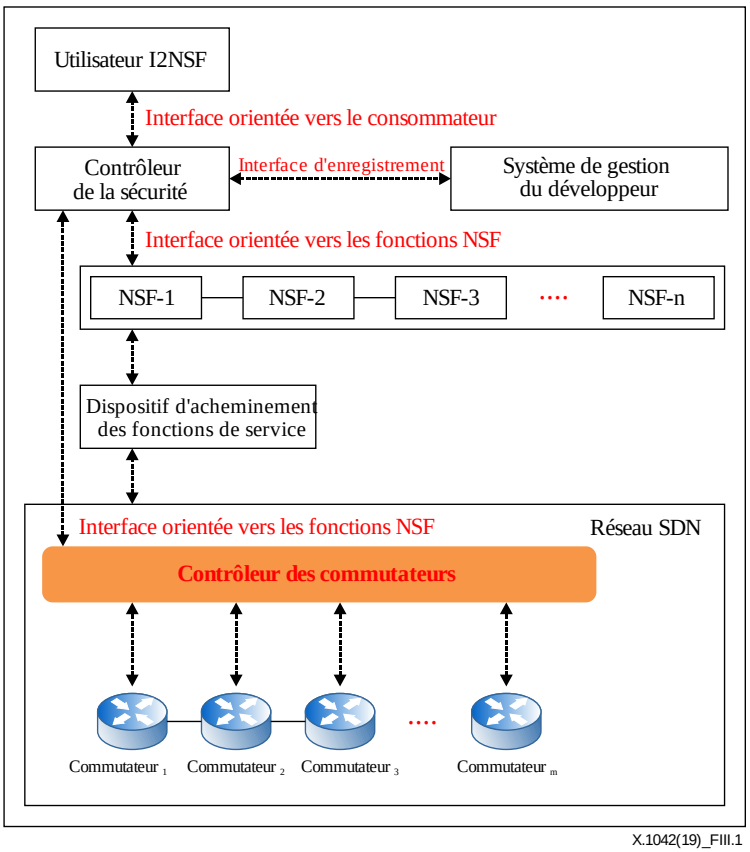


Figure III.1 – Cadre de l'IETF pour l'interface avec la fonction de sécurité de réseau

III.1.2 Comparaison entre l'architecture de l'IETF et celle de l'UIT-T

La Figure III.2 montre la comparaison entre le cadre I2NSF reposant sur les réseaux SDN et l'architecture de l'UIT-T. Les composants de l'UIT-T sont indiqués en bleu.

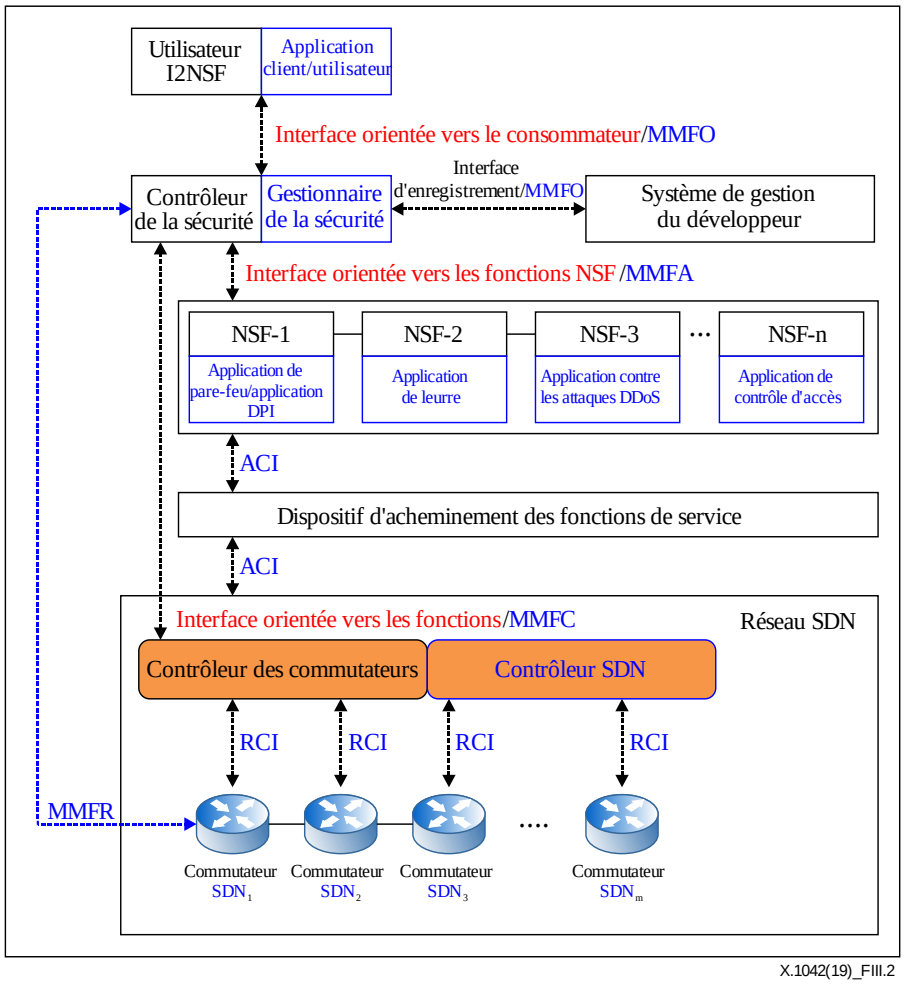


Figure III.2 – Comparaison entre l'architecture de l'IETF et celle de l'UIT-T

III.2 Architecture SDN de l'ONF

III.2.1 Aperçu général

Le présent paragraphe décrit l'architecture SDN de l'ONF. La Figure III.3 illustre l'architecture SDN figurant dans [b-ONF TR521]. Dans cette Figure, le réseau SDN est modélisé par un ensemble de relations client-serveur entre les contrôleurs SDN et d'autres entités, qui peuvent aussi être des contrôleurs SDN. En tant que serveur, un contrôleur SDN peut fournir des services à un nombre quelconque de clients et, en tant que client, il peut demander des services à un nombre quelconque de serveurs. Dans la mesure où leur interface présente un comportement approprié, les détails internes des entités autres que les contrôleurs SDN n'entrent pas dans le cadre de cette architecture. Dans ce qui suit, on utilisera le protocole OpenFlow.

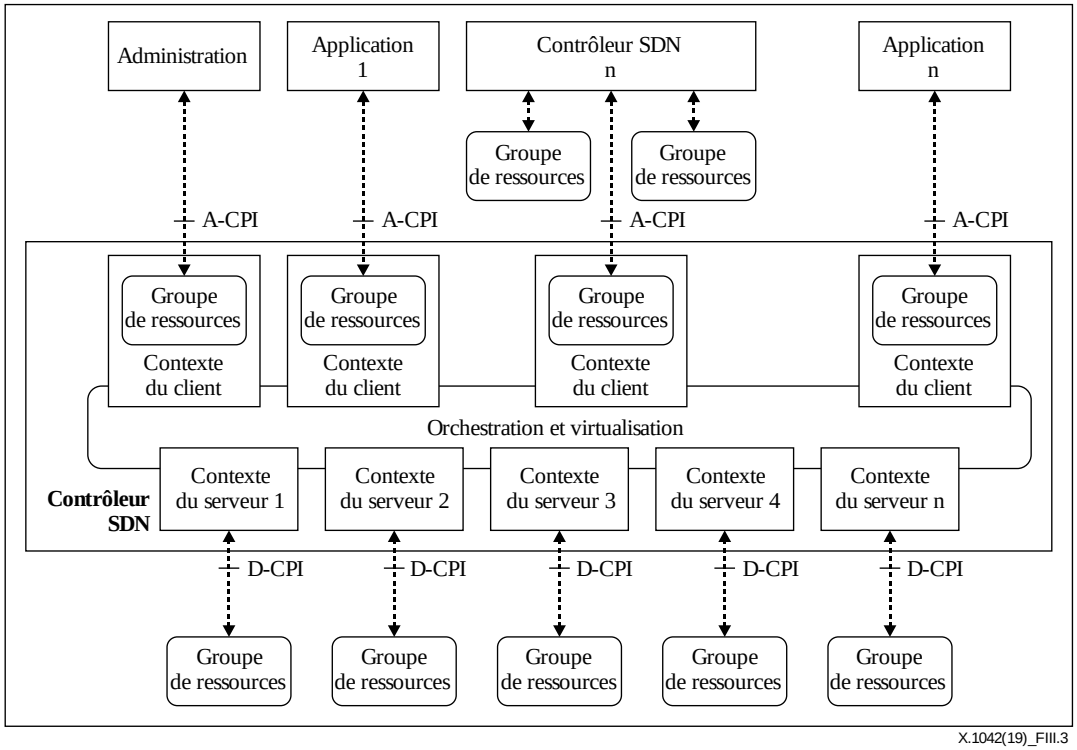


Figure III.3 – Architecture SDN de l'ONF

III.2.2 Comparaison entre l'architecture de l'ONF et celle de l'UIT-T

La Figure III.4 montre la comparaison entre l'architecture de l'ONF et celle de l'UIT-T. Les composants de l'UIT-T sont indiqués en bleu.

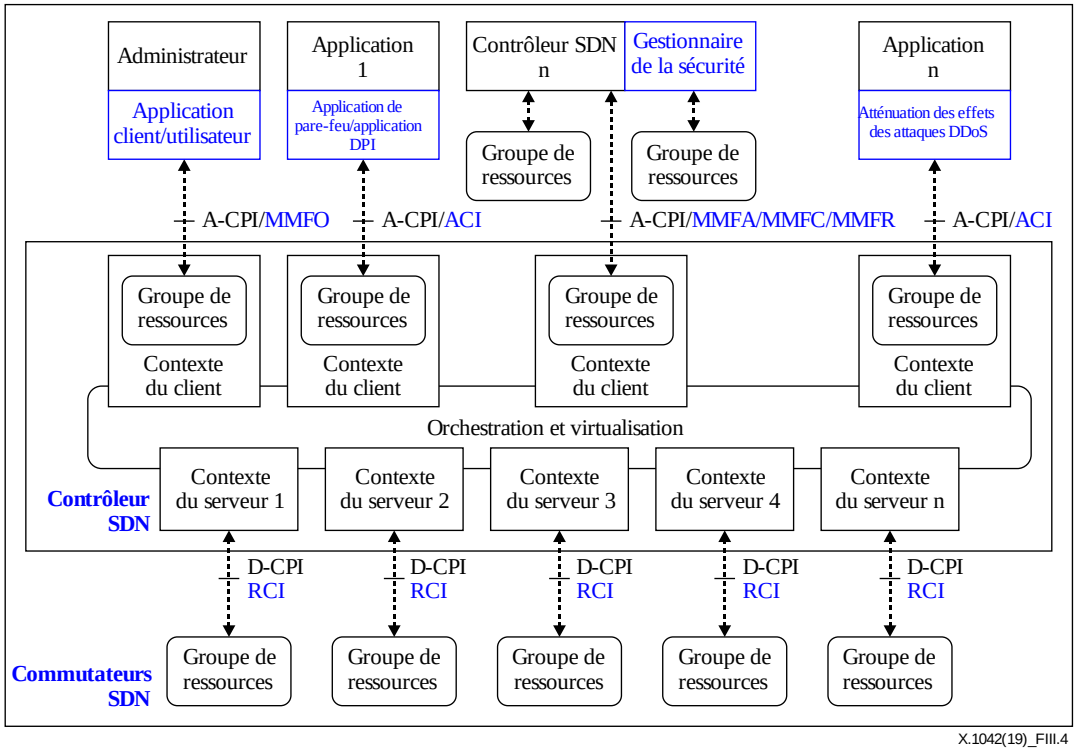


Figure III.4 – Comparaison entre l'architecture de l'ONF et celle de l'UIT-T

Bibliographie

[b-UIT-T X.812] Recommandation UIT-T X.812 (1995) | ISO/CEI 10181-3:1996 *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre de contrôle d'accès*.

[b-UIT-T X.1252] Recommandation UIT-T X.1252 (2010), *Termes et définitions de base relatifs à la gestion d'identité*.

[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

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	**Réseaux de données, communication entre systèmes ouverts et sécurité**
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2019