International Telecommunication Union

ITU-T X.1042

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(01/2019)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Network security

Security services using software-defined networking

Recommendation ITU-T X.1042

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	**X.1030–X.1049**
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1042

Security services using software-defined networking

Summary

Recommendation ITU-T X.1042 supports the protection of network resources using security services based on software-defined networking (SDN). This Recommendation first classifies the network resources for SDN-based security services: SDN application, SDN controller, SDN switch and security manager (SM). Recommendation ITU-T X.1042 then defines security services based on SDN.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1042	2019-01-30	17	11.1002/1000/13803

Keywords

Access control, DDoS attack, firewall, honeypot, software-defined networking (SDN), security scenarios.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g.,, interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1042

Security services using software-defined networking

1 Scope

This Recommendation supports the protection of network resources using security services based on software-defined networking (SDN). This Recommendation covers:

– classification of the network resources that can be protected by SDN-based security services;

– definition of security services based on SDN;

– specification of the implementation of SDN-based security services.

The protection of network resources (e.g., router, switch, firewall and intrusion detection system) by SDN-based security services means:

– prompt reaction to new network attacks [e.g., worms and distributed denial-of-service (DDoS) attacks];

– construction of private networks to mitigate sophisticated network attacks;

– automatic defence from network attacks without the intervention of network administrators;

– dynamic network-load-aware resource allocation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T Y.3300] Recommendation ITU-T Y.3300 (2014), *Framework of software-defined networking.*

[ITU-T Y.3301] Recommendation ITU-T Y.3301 (2016), *Functional requirements of software-defined networking.*

[ITU-T Y.3302] Recommendation ITU-T Y.3302 (2017), *Functional architecture of software-defined networking.*

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 software-defined networking [ITU-T Y.3300]: A set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner.

3.1.2 access control [b-ITU-T X.1252]: A procedure used to determine if an entity should be granted access to resources, facilities, services, or information based on pre-established rules and specific rights or authority associated with the requesting party.

3.1.3 access control policy [b-ITU-T X.812]: The set of rules that define the conditions under which an access may take place.

3.1.4 access control policy rules [b-ITU-T X.812]: Security policy rules concerning the provision of the access control service.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 network resource: A device that performs packet forwarding in a network system.

NOTE – Network resources include network switches, routers, gateways and WiFi access points.

3.2.2 firewall: A device or service at the junction of two network segments that inspects every packet that attempts to cross the boundary. It also rejects any packet that is disqualified by certain criteria, such as the presence of disallowed port numbers or IP addresses.

NOTE – Firewall services can be separated from physical devices and work as an application.

3.2.3 honeypot: A computer security mechanism set up as a decoy to lure cyber attackers. It is used to detect or deflect attacks from legitimate target, and to collect attack data. The term honeypot comes from its behaviour, which attracts attackers ("bees") to a place (the attack target, or "honey") used as a trap.

3.2.4 centralized firewall service: A service that can establish and distribute access control policy rules into network resources for efficient firewall management. These rules can be managed dynamically by a centralized server. Software-defined networking (SDN) can work as a centralized firewall service through a standard interface between firewall applications and network resources.

3.2.5 centralized DDoS attack mitigation service: A service that can establish and distribute access control policy rules into network resources for efficient distributed denial-of-service (DDoS) attack mitigation. These rules can be managed dynamically by a centralized server. Software-defined networking (SDN) can work as a centralized DDoS attack mitigation service through a standard interface between DDoS attack mitigation applications and network resources.

3.2.6 centralized honeypot service: A service that can establish and distribute access control policy rules into network resources for the dynamic honeypot configuration. These rules can be managed dynamically by a centralized server. Software-defined networking (SDN) can work as a centralized honeypot service through a standard interface between honeypot applications and network resources.

3.2.7 centralized illegal device management service: A service that can establish and distribute access control policy rules into network resources for the blacklist of illegal devices. These rules can be managed dynamically and globally by a centralized server. Software-defined networking (SDN) can work as network-based illegal device management through a standard interface between illegal device management applications and network resources.

NOTE – A criterion for an illegal device lies outside the scope of this Recommendation. An example of the illegal device may be determined according to usage of the global unique identification system.

3.2.8 access control management service: A service that can establish and distribute access rights policies into network resources for the whitelist of Internet of things (IoT) devices. These policies can be managed dynamically and globally by a centralized server. Software-defined networking (SDN) can work as network-based IoT device management through a standard interface between access control management applications and network resources.

NOTE – Specification of a hierarchical composition of access policies lies outside the scope of this Recommendation. These access policies may be composed and divided according to the security level of network resources and distributed into the network system.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACI	Application Control Interface
ACM	Access Control Management
AL-MSO	Application Layer Management Support and Orchestration
ALM	Application Layer Management
BSS	Business Support System
CL-AS	Control Layer Application Support
CL-CLS	Control Layer Control Layer Service
CL-MSO	Control Layer Management Support and Orchestration
CL-RA	Control Layer Resource Abstraction
CLM	Control Layer Management
DDoS	Distributed Denial-of-Service
DNS	Domain Name Service
DPI	Deep Packet Inspection
I2NSF	Interface to Network Security Function
IoT	Internet of Things
IP	Internet Protocol
MAC	Media Access Control
MMF	Multi-layer Management Function
MMFA	Multi-layer Management Function Application layer
MMFC	Multi-layer Management Function Control layer
MMFO	Multi-layer Management Function OSS/BSS
MMFR	Multi-layer Management Function Resource layer
NSF	Network Security Function
OSS	Operation Support System
RCI	Resource Control Interface
RLM	Resource Layer Management
RL-MS	Resource Layer Management Support
SDN	Software-Defined Networking
SDN-AL	Software-Defined Networking – Application Layer
SDN-CL	Software-Defined Networking – Control Layer
SDN-RL	Software-Defined Networking – Resource Layer
SIP	Session Initiation Protocol
SM	Security Manager
TCP	Transmission Control Protocol
VoIP	Voice over Internet Protocol

VoLTE Voice over Long-Term Evolution

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "is prohibited from" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview of the SDN functional architecture

This clause describes the high-level reference architecture for security services (e.g., firewall and DDoS attack mitigation) using the SDN high-level architecture of [ITU-T Y.3300], such as the centralized firewall service and centralized DDoS attack mitigation service.

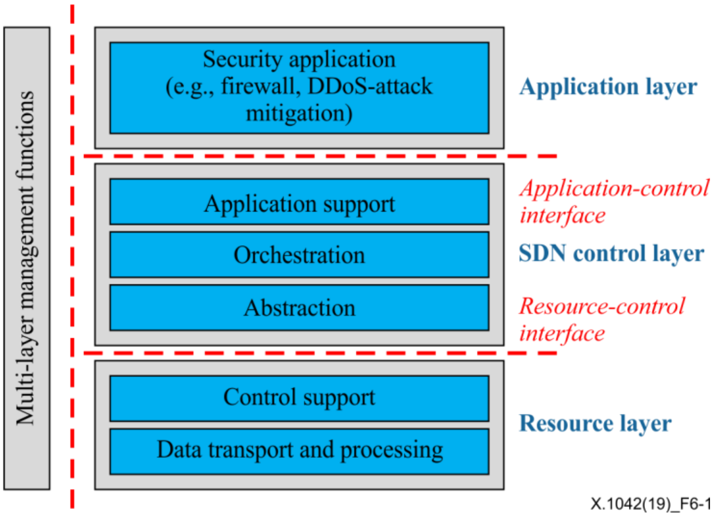

Multi-layer management functions
Security application (e.g., firewall, DDoS-attack mitigation)
Application layer
Application-control interface
Application support
Orchestration
Abstraction
SDN control layer
Resource-control interface
Control support
Data transport and processing
Resource layer
X.1042(19)_F6-1

Figure 6-1 – High-level architecture for SDN-based security services

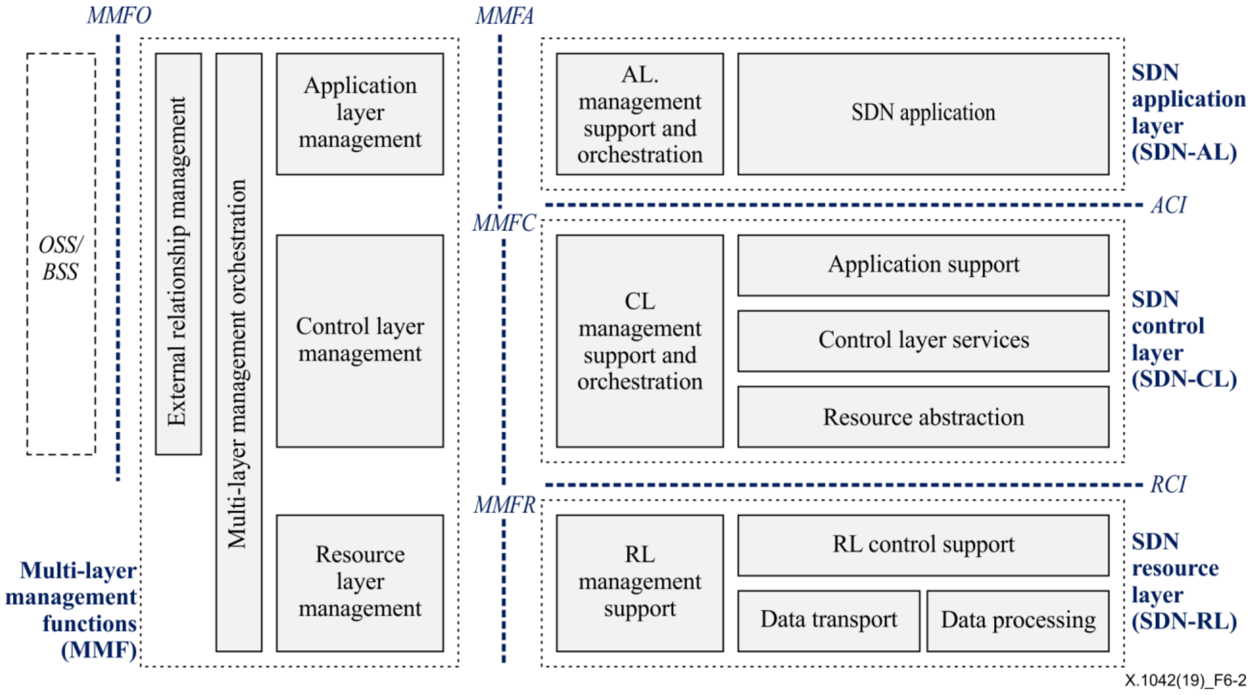
As shown in Figure 6-1, applications for security services (e.g., firewall, DDoS attack mitigation and honeypot services) run on top of the SDN architecture. When a user or an administrator (e.g., application layer management (ALM) in Figure 6-2) enforces security policies for the security services through an application interface, the SDN controller generates the corresponding access control rules to meet such security policies in an autonomous and prompt manner. According to the access control rules generated, network resources, such as SDN switches, act to mitigate network attacks, for example, by dropping packets with suspicious patterns.

Figure 6-2 shows the functional architecture of SDN in [ITU-T Y.3302], which is based on the high-level architecture of SDN.

– Software-defined networking – application layer (SDN-AL): The SDN-AL is composed of ALM support and orchestration (AL-MSO) functional component and multiple SDN application functional components [ITU-T Y.3302]. The AL-MSO interacts with the ALM functional component in multi-layer management function (MMF) via the multi-layer management function application layer (MMFA) reference point in order to support management of SDN applications and to enable joint operations of management in all SDN sub-layers. SDN applications interact with the software-defined networking – control layer (SDN-CL) via the application control interface (ACI) reference point with requests for the SDN-CL to automatically customize the behaviour and properties of network resources. SDN applications use the abstracted view and status of the network resources that are provided by the SDN-CL by means of information and data models exposed through the ACI reference point. Depending on the SDN use cases (e.g., intra or inter data centres, mobile networks, access networks), different ACIs can optionally be defined. It is assumed that ACIs use open application programming interfaces.

– SDN-CL: The SDN-CL is composed of control layer management support and orchestration (CL-MSO), control layer application support (CL-AS), control layer control layer services (CL-CLSs) and control layer resource abstraction (CL-RA). The SDN-CL provides programmable means to control the behaviour of SDN resources, e.g., data transport and processing resources, according to SDN-AL requests and MMF policies. The SDN-CL operates on resources provided by the software-defined networking – resource layer (SDN-RL) and exposes an abstracted view of the network to the SDN-AL. The SDN-CL interacts with SDN-RL using a resource control interface (RCI) reference point, with a control layer management (CLM) functional component in MMF using the multi-layer management function control layer (MMFC) reference point. It also interacts with the SDN-AL using an ACI reference point. The CL-MSO may request the MMF to delegate some management functions. The MMF provide functionalities for managing the functionalities of the SDN-CL through the MMFC reference point.

– SDN-RL: The SDN-RL is composed of resource layer management support (RL-MS), resource layer control support, resource layer data processing and resource layer data transport. The SDN-RL is where the physical or virtual network elements perform transport or processing of data packets according to SDN-CL decisions. The policy-provisioning information (including configuration information) that results as decisions made by the SDN-CL, as well as information about network resources, are exchanged via the RCI reference point. Information exchanged through the RCI includes control information provided by the SDN-CL to the SDN-RL, e.g., for configuring a network resource or providing policies, as well as the information that pertains to the notifications sent by the SDN-RL whenever a network resource change is detected (if such information is available). The RL-MS provides a resource description, i.e., vendor, software version and their status (e.g., central processing unit load, random access memory used or storage). It may include a management agent that performs some local management operations, if delegated by the MMF. The MMF provides functionalities for managing the functionalities of SDN-RL through the multi-layer management function resource layer (MMFR) reference point.


MMFO
MMFA
OSS/ BSS
External relationship management
Multi-layer management orchestration
Application layer management
Control layer management
Resource layer management
Multi-layer management functions (MMF)
AL. management support and orchestration
SDN application
SDN application layer (SDN-AL)
ACI
MMFC
CL management support and orchestration
Application support
Control layer services
Resource abstraction
SDN control layer (SDN-CL)
RCI
MMFR
RL management support
RL control support
Data transport
Data processing
SDN resource layer (SDN-RL)
X.1042(19)_F6-2

BSS: business support system; MMFO: multi-layer management function OSS/BSS; OSS: operation support system

Figure 6-2 – SDN functional architecture [ITU-T Y.3302]

7 Classification of network resources

This clause defines four network resources for security services using SDN based on Figure 6-2.

1) SDN application. A service that explicitly, directly and programmatically communicates its network requirements and desired network behaviour to the SDN controller via a northbound interface such as the ACI in Figure 6-2. In addition, SDN applications may consume an abstracted view of the network for their internal decision-making purposes. For example, firewall, honeypot, DDoS mitigation and illegal device management services can be provided as applications. These SDN applications are required to interact with the ALM through the AL-MSO for fault, configuration, accounting, performance and security management. In addition, these applications make access rules, thus they are also required to interact with the SDN-CL via ACIs so that access rules are implemented.

2) SDN controller. A logically centralized entity in charge of: i) translating the requirements from SDN applications to SDN switches; and ii) providing abstract network views to applications with useful network information, e.g., traffic statistics and events. In other words, an SDN controller creates flow entries based on access rules it gets from SDN applications. Therefore, the SDN controller is required to interact with the CLM, SDN applications and the SDN-RL.

3) SDN switch. A software program or hardware device that forwards packets in an SDN environment. SDN switches are capable of storing packet forwarding rules managed by an SDN controller via a southbound interface such as RCI in Figure 6-2. So, the SDN switch is required to interact with the resource layer management (RLM) and the SDN-CL.

4) Security manager (SM). An ALM function that transfers security policies to an SDN application. So, the SM is required to interact with SDN applications through the AL-MSO. Figure 7-1 shows the location of network resources in Figure 6-2. These network resources are required to follow the requirements of [ITU Y.3301].

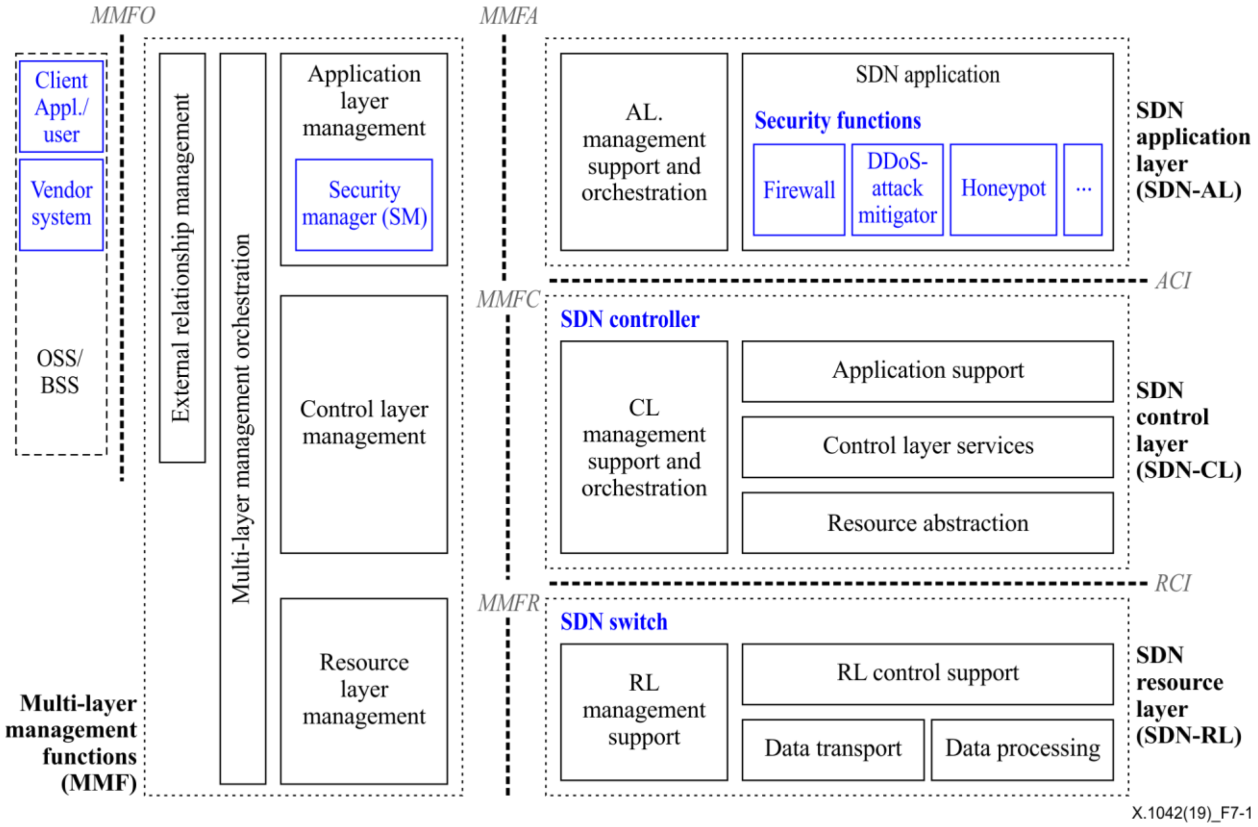


Figure 7-1 – Network resources in SDN-based security services

8 Security services based on SDN

This clause introduces security services using SDN in two kinds of networking: i) intra-domain networking, e.g., centralized firewall service and centralized honeypot service; and ii) inter-domain networking, e.g., centralized DDoS attack mitigation service and centralized illegal device management service. The domain in this Recommendation refers to a group of network resources that is administered with common rules and procedures.

8.1 Centralized firewall service

8.1.1 Basic concept of centralized firewall service

This clause describes the basic concept of a centralized firewall service. This service can manage network resources so that firewall rules can be managed flexibly. As shown in Figure 8-1, a centralized firewall manages SDN switches and firewall rules can be inserted into or deleted from them.

NOTE – It is easy to convert a packet-filtering strategy issued by the firewall application to a flow table through the controller. However, a protocol between controller and switches (e.g., OpenFlow and NETCONF protocols) is currently only able to match up to the transmission control protocol (TCP) layer and there is no corresponding field to set the identification information of a data packet above the TCP layer. So a firewall strategy to identify information above the TCP layer cannot be achieved without changing the protocol.

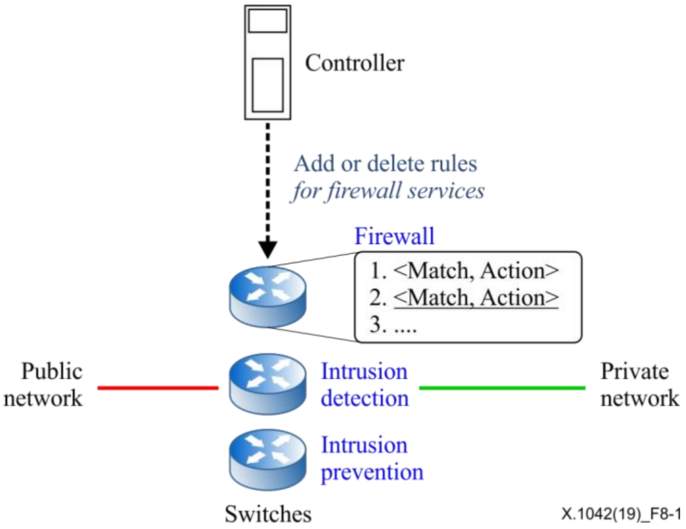


Figure 8-1 – Concept of centralized firewall services

8.1.2 Service scenario of centralized firewall service

Figure 8-2 shows an example scenario of a centralized firewall service to stop a worm spreading.

As a precondition for this scenario, an SM should specify a new policy to the firewall application when the information about a new worm is recognized. In order to prevent packets including this worm from spreading, the user could add the new policy (e.g., "drop packets with the worm file") to the firewall application running on top of the SDN controller. It can also be managed centrally, so that an SM might determine security policies for a firewall application through a single point, i.e., an SDN controller.

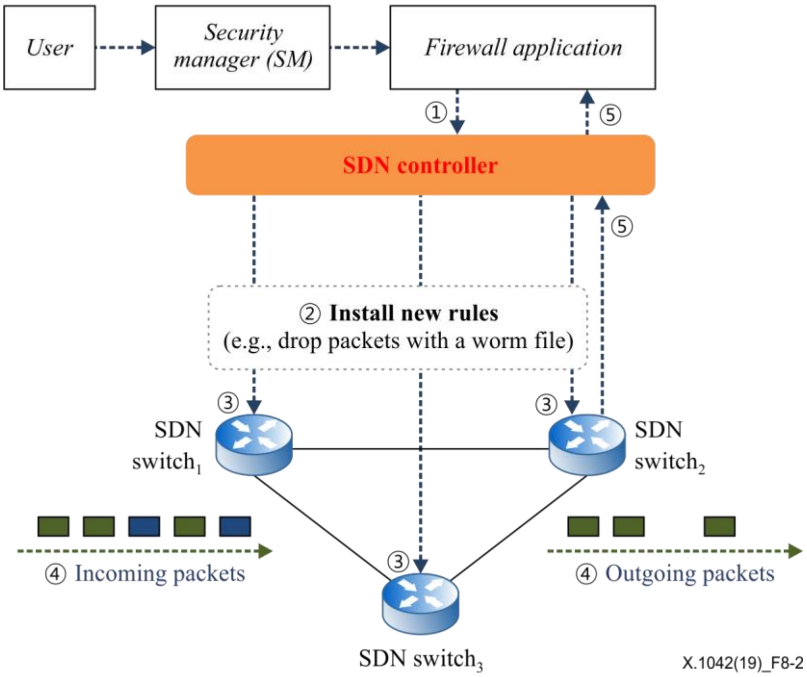


Figure 8-2 – Intra-domain scenario of a centralized firewall service

– Step 1. A firewall application installs new rules.

A firewall application should specify a new rule when the information about a new worm is reported. The new rule (e.g., "Drop packets with the worm file") is added to the SDN controller.

– Step 2. The SDN controller distributes a new flow entry to all SDN switches.

A new flow entry might be distributed to each switch by an SDN controller after installing it. Therefore, the SDN controller sends a flow insert operation that contains the rule (e.g., "Drop packets with the worm file") to all SDN switches.

The reported new worm in this clause is either a known worm or a "zero-day" worm. As for a known worm, some mechanisms, e.g., signatures or thumbprints, are developed in a firewall service to detect and defend it. However, a zero-day worm should be scanned and detected before any countermeasure is applied to defend against it. Worms deliver malicious payloads that could exploit some vulnerable applications or services. Those worms might be detected by inspecting the packet payload. An example of packet data scan detection is shown in Appendix II.

– Step 3. All SDN switches insert the new flow entry into their flow table.

An SDN switch adds a flow entry dropping future packets with the worm file to its flow table when receiving the flow insert operation about the worm file. After that, the SDN switch can drop the packets with the worm file.

– Step 4. The SDN switch executes flow entries to drop packets including worm files.

An SDN switch completely drops packets when receiving packets with a worm file. Any packets with a worm file cannot be passed under applied rules.

– Step 5. An SDN switch reports to a controller when receiving an unfamiliar packet.

When an SDN switch receives a type of packet that it has never processed before, it deletes this packet and sends a report to the controller about this kind of packet. The controller analyses whether this is an attack. If this is an attack, the controller sends a message to the firewall application and step 1 will be executed. If not, the controller keeps a regular flow entry to tell switches how to handle this sequence for subsequent packets.

8.1.3 Service scenario of a collaborated firewall service

Figure 8-3 shows an example scenario of a collaborated firewall application with a deep packet inspection (DPI) application to achieve centralized voice over internet protocol (VoIP)/voice over long-term evolution (VoLTE) flow monitoring and management. This scenario shows that the DPI application controls each SDN switch for VoIP/VoLTE call flow management by manipulating rules that can be added, deleted or modified dynamically. This application can cooperate with a firewall application to protect the VoIP/VoLTE service. Specifically, a firewall-enabled switch performs basic security checks of packets of unknown flows. If the switch detects that the packet is an unknown VoIP call flow packet that exhibits some suspicious patterns, then it triggers the SDN controller for more specialized security analysis of the suspicious VoIP call packet.

As a precondition for this scenario, an SM should specify a new policy to the firewall and DPI application when the information about a suspicious pattern is recognized. In order to prevent packets from including these patterns, the user adds the new policy (e.g., "drop packets with suspicious patterns") to the firewall and the DPI application running on top of the SDN controller. It can also be managed centrally, so that an SM might determine security policies for applications through a single point, i.e., an SDN controller.

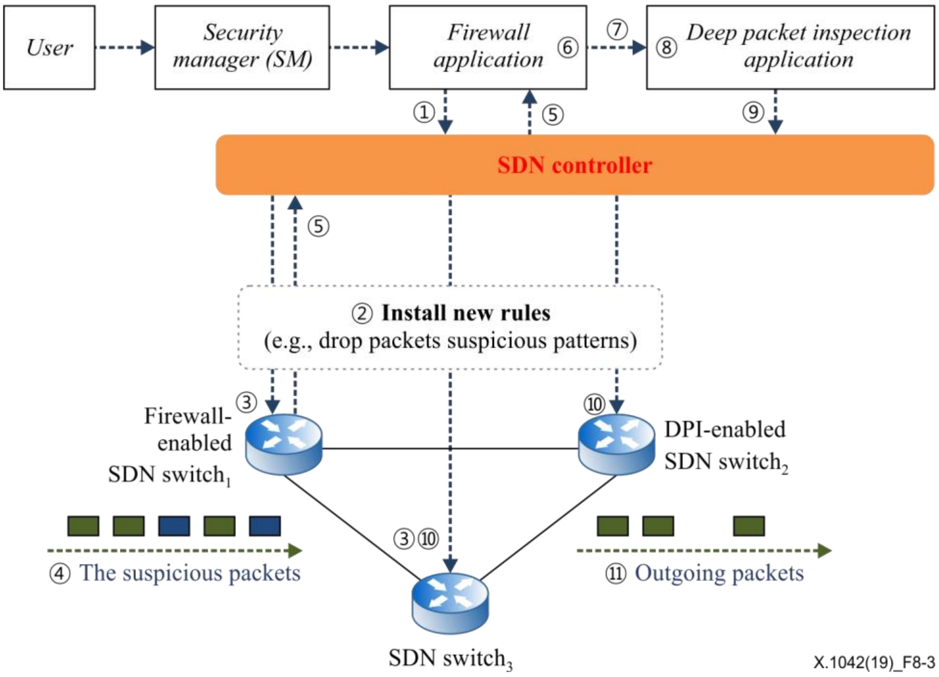


Figure 8-3 – Intra-domain scenario of collaborated firewall service

– Step 1. Firewall and DPI applications install new rules for well-known pattern.

Firewall and DPI applications should specify a new rule when the information about a new pattern is reported. The new rule (e.g., deliver packets with the pattern to the SDN controller) is added to the SDN controller.

– Step 2. The SDN controller distributes a new flow entry to all SDN switches.

A new flow entry might be distributed to each switch by an SDN controller. Therefore, the SDN controller sends a flow insert operation that contains the rule (e.g., deliver packets with the pattern) to all SDN switches. If each switch has a different function, the SDN controller sends different flow entries into each. That is, the firewall-enabled switches should not get the DPI-related flow entries.

– Step 3. All SDN switches insert the new flow entry into their flow tables.

An SDN switch adds a flow entry in order to deliver future packets with the suspicious pattern to its flow table when receiving the flow insert operation from the SDN controller.

– Step 4. The SDN switch executes flow entries to deliver packets including suspicious patterns.

An SDN switch delivers packets when receiving packets with a suspicious pattern into the SDN controller. All packets with suspicious patterns should be transferred to the SDN controller under applied rules.

– Step 5. The SDN switch and controller forwards on receipt any unfamiliar packet to the firewall application.

When an SDN controller receives a type of packet that it has never processed before, it forwards these packets to the firewall application for basic security inspection.

– Step 6. The firewall application analyses the unfamiliar packet.

The firewall application analyses the header fields of the packet and determines that this is an unknown VoIP call flow signal packet, e.g., a session initiation protocol (SIP) packet, of a suspicious pattern.

– Step 7. The firewall application triggers the DPI application.

The firewall application triggers an appropriate application, e.g., a DPI application, for detailed security analysis of the suspicious signal packets. After that, it forwards the packets to the DPI application.

– Step 8. The DPI application analyses the unfamiliar packet.

The DPI application analyses the headers and contents of the signal packet, e.g., calling number and session description headers. If, for example, the DPI application regards the packet as spoofed by hackers or a scanning packet searching for VoIP/VoLTE devices, it drops the packet.

– Step 9. The DPI application requests the SDN controller to block that packet.

The DPI application requests the SDN controller to block that packet and the subsequent packets that have the same call identifier.

– Step 10. The SDN controller installs new rules.

The SDN controller distributes a new flow entry (e.g., "drop the packets") to all SDN switches, as in step 2. After that, all illegal packets will be dropped by these switches.

8.2 Centralized honeypot service

8.2.1 Basic concept of a centralized honeypot service

This clause describes the basic concept of a centralized honeypot service. The honeypot can dynamically manage honeypot places. As shown in Figure 8-4, a centralized honeypot manages switches and new routing paths to attract attackers to a place used as a trap, i.e., a honeypot. The honeypot is configured as the intended attack target and reports the collected information to the centralized honeypot service.

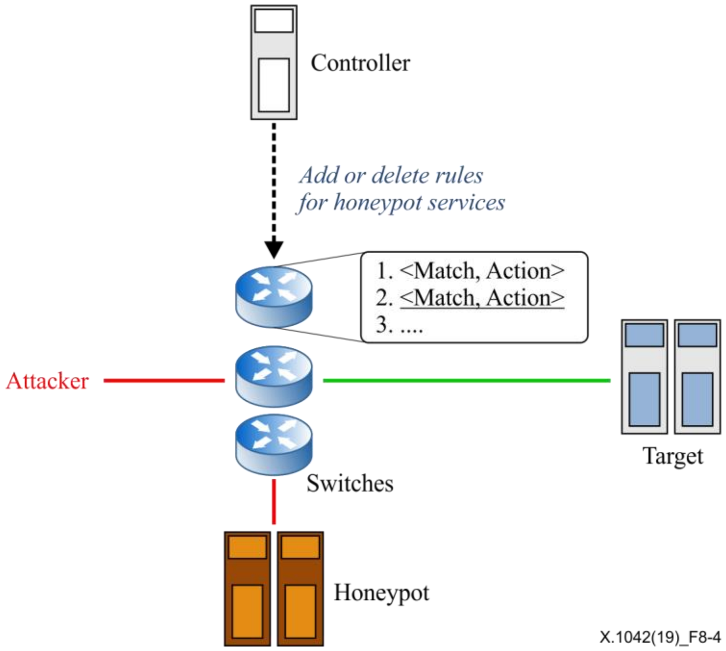


Figure 8-4 – Concept of centralized honeypot service

8.2.2 Service scenario of a centralized honeypot

Figure 8-5 shows an example scenario of a centralized honeypot service to add a routing path to a honeypot instead of the actual target for SDN switches.

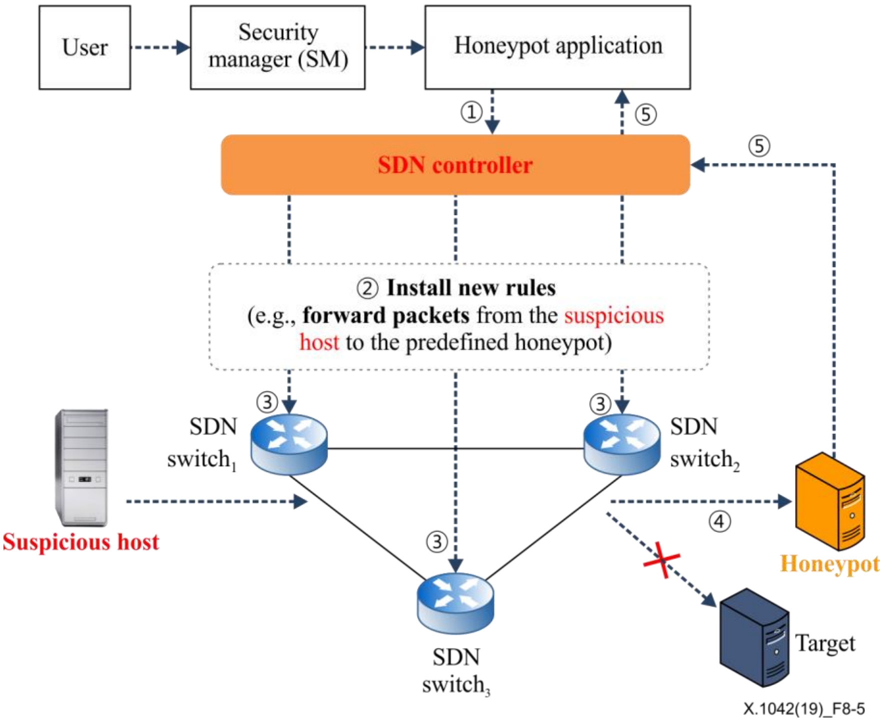


Figure 8-5 – Intra-domain scenario for a centralized honeypot service

– Step 1. A honeypot application installs new rules on the SDN controller.

A honeypot application should specify a new rule when information about a suspicious host is reported. In order to monitor traffic from a suspicious host, the new rule (e.g., "Forward packets from the suspicious host to a honeypot") is added to the SDN controller by the honeypot application running on top of the SDN controller.

– Step 2. An SDN controller distributes new rules to appropriate SDN switches.

A new rule might be distributed to each switch by an SDN controller after installing it. Therefore, the SDN controller sends a flow insert operation that contains the rule (e.g., "Forward packets from the suspicious host to a honeypot") to all SDN switches. It can also be managed centrally, so that an SM can determine security policies for their service through a single point, i.e., an SDN controller.

– Step 3. All SDN switches insert new rules into their flow tables.

All SDN switches add a flow entry forwarding future packets from the suspicious host to a honeypot to their flow tables when receiving the flow insert operation about the suspicious host. After that, the SDN switch can forward the packets from the suspicious host to a honeypot.

– Step 4. An SDN switch executes new rules to support the honeypot service.

An SDN switch can forward the packets to a honeypot when receiving packets from the suspicious host. Any packets from the suspicious host cannot be passed to an actual target host switch under applied rules. The forwarded packets are collected in the honeypot.

– Step 5. Honeypot service reports to controller about suspicious packets.

When a honeypot service receives packets from suspicious hosts, it processes these packets and sends a report to the controller about this kind of packet to support the packet analysis of the controller.

8.3 Centralized DDoS attack mitigation service

8.3.1 Basic concept of a centralized DDoS attack mitigation service

Figure 8-6 shows a centralized DDoS attack mitigation service. This service adds to, deletes from or modifies rules for each SDN switch. Unlike the centralized firewall service related to the intra-domain, this service mainly focuses on the inter-domain.

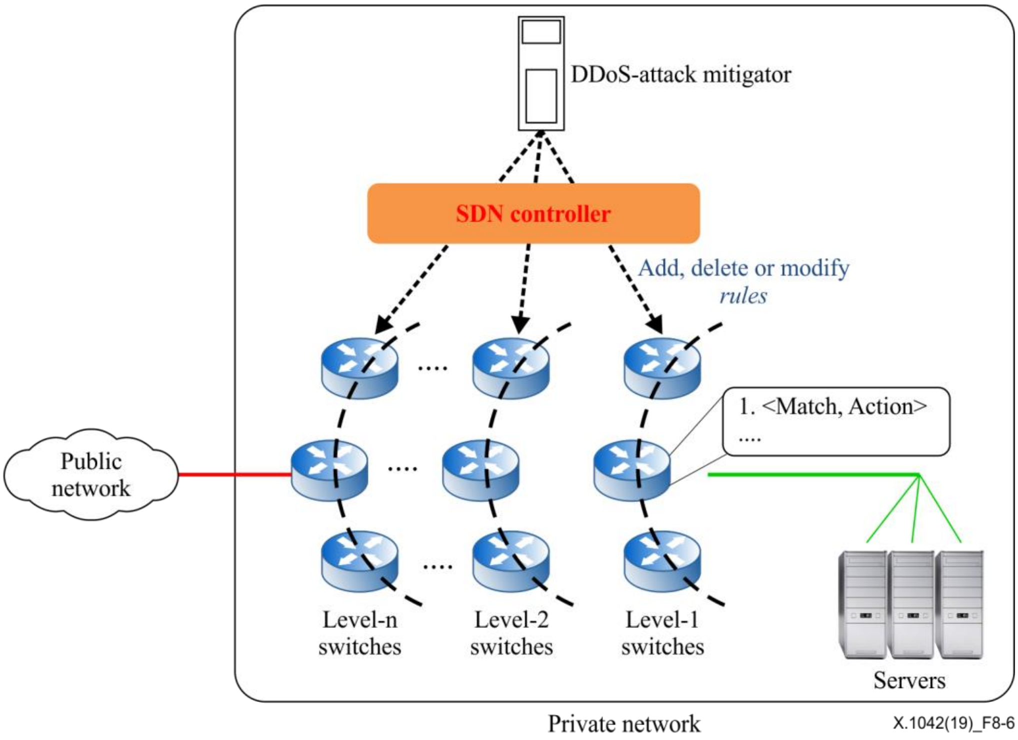


Figure 8-6 – Concept of centralized DDoS attack mitigation services

8.3.2 Centralized DDoS attack mitigation service for stateless servers

Figure 8-7 shows an example scenario of a centralized DDoS attack mitigation service for stateless domain name service (DNS) servers.

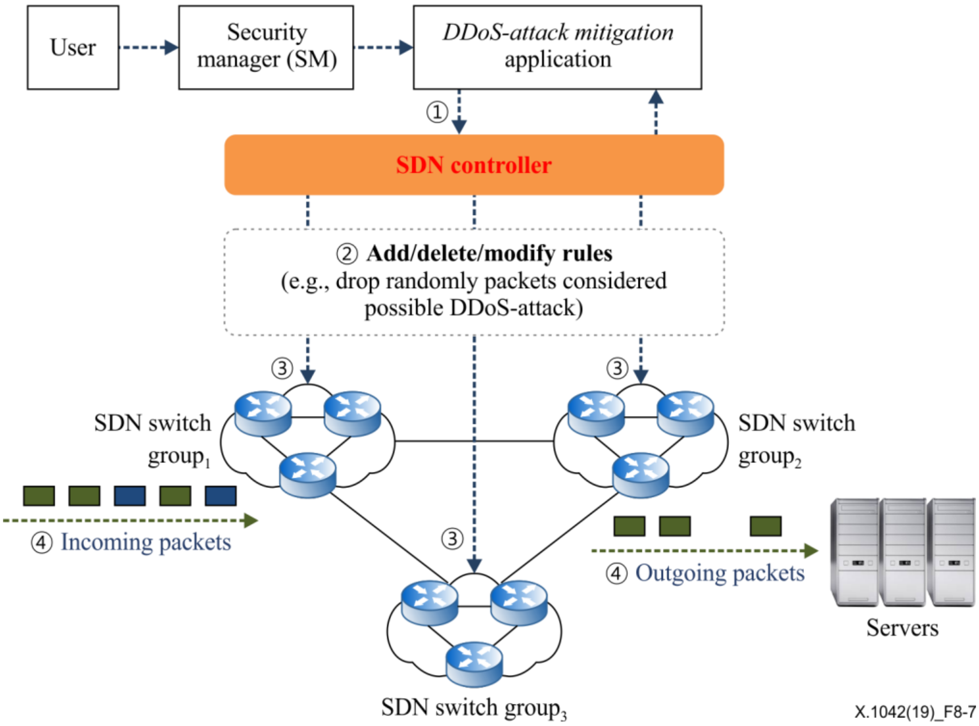


Figure 8-7 – Inter-domain scenario for a centralized DDoS attack mitigation service for stateless servers

– Step 1. A mitigation application installs new rules for the SDN controller.

A DDoS attack mitigation application should specify a new rule when a new DDoS attack is known from the SM. In order to prevent packets from reaching servers and wasting server resources, the new rule (e.g., "Drop DDoS attack packets randomly with some probability") is added to the SDN controller. This rule addition is performed by DDoS attack mitigation application running on top of the SDN controller.

– Step 2. An SDN controller distributes new rules to the appropriate switches.

A new rule might be distributed to each switch by an SDN controller after installing it. Therefore, the SDN controller sends a flow insert operation that contains the rule (e.g., "Drop randomly packets considered DDoS attacks with a certain probability") to all SDN switches. It can also be managed centrally, so that an SM can determine security policies for their service through a single point, i.e., an SDN controller.

– Step 3. All SDN switches insert new rules into their flow tables.

All SDN switches add a flow entry dropping future packets considered to be DDoS attack packets to their flow tables when receiving the flow insert operation about DDoS attack mitigation. After that, an SDN switch among switches in the domain can drop DDoS attack packets with a probability proportional to the severity of the DDoS attack.

– Step 4. An SDN switch executes new rules to mitigate DDoS attack.

An SDN switch completely drops packets selectively when receiving DDoS attack packets. DDoS attack packets are dropped randomly through SDN switches in each domain according to the processing capabilities and the features of domains. Thereafter, drop results should be reported to the SDN controller.

8.3.3 Centralized DDoS attack mitigation service for stateful servers

Figure 8-8 shows an example scenario of centralized DDoS attack mitigation for stateful web servers.

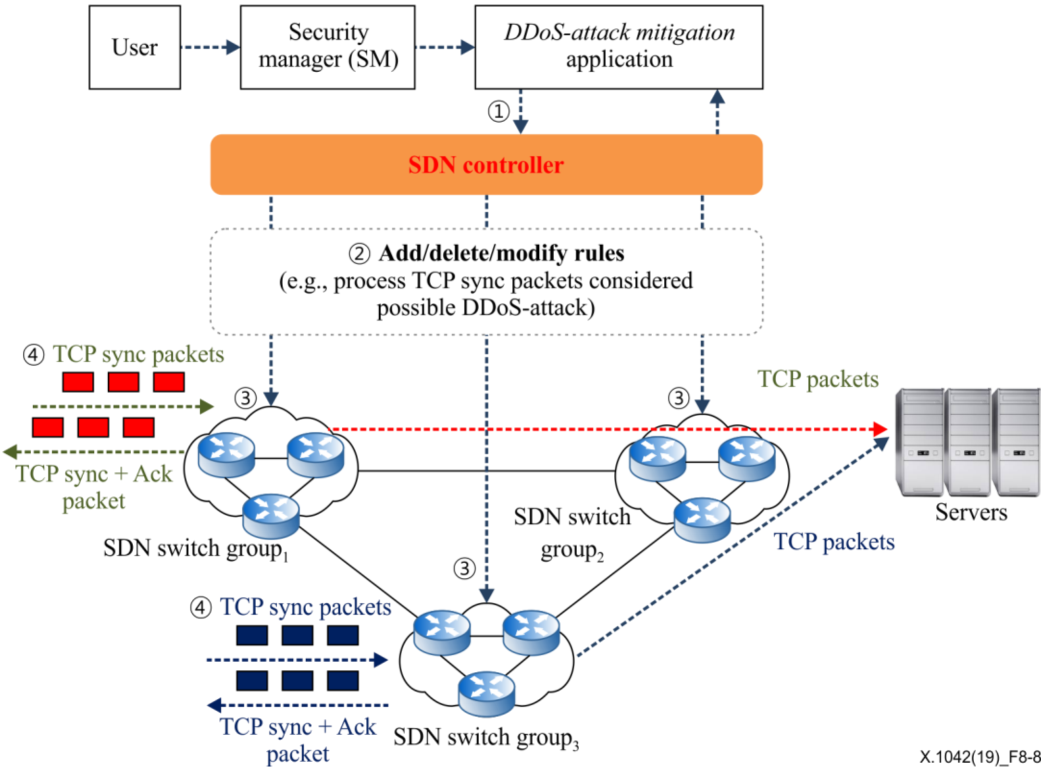


Figure 8-8 – Inter-domain scenario for centralized DDoS attack mitigation for stateful servers

– Step 1. A mitigation application installs new rules for the SDN controller.

A DDoS attack mitigation application should select which switch performs the role of proxy for the TCP service. New rule addition is performed by the DDoS attack mitigation application running on top of the SDN controller.

– Step 2. An SDN controller distributes new rules to the appropriate switches.

A new rule might be distributed to appropriate switches for DDoS attack mitigation by an SDN controller after installing it. Therefore, the SDN controller sends a flow insert operation that contains the rule (e.g., "Generate TCP Sync+Ack for packets considered to be DDoS attacks") to all SDN switches. Therefore, a new rule is installed into the selected switch so that it can generate TCP Sync-Ack packets for TCP Sync as requests. If the same requests arrive much more frequently than expected, the SDN controller selects a new switch so that the switch behaves in the role of the server. For the normal TCP Sync, the switch transfers the TCP session to the corresponding server in the private network. It can also be managed centrally, so that an SM can determine security policies for their service through a single point, i.e., the SDN controller.

– Step 3. All SDN switches apply to new rules in their flow table.

All SDN switches add a flow entry dropping future packets considered to be DDoS attack packets to their flow table when receiving the flow insert operation about DDoS attacks. After that, the SDN switch can generate TCP Sync-Ack packets with a probability proportional to the severity of the DDoS attack.

– Step 4. An SDN switch executes new rules to mitigate the DDoS attack.

An SDN switch completely responds to TCP Sync packets from an adversary host randomly when receiving DDoS attack packets. DDoS attack requests for stateful servers are handled by switches instead of actual servers. Then, the execution result of the SDN switch to mitigate the DDoS attack should be transmitted to the SDN controller.

8.4 Centralized illegal device management service

8.4.1 Basic concept of a centralized illegal device management service

This clause describes the basic concept of a centralized illegal device management service. As shown in Figure 8-9, a centralized illegal device management service manages the backlist of illegal devices to prevent traffic from those devices. The list of illegal devices is stored in a blacklist database and can be updated either manually or automatically by independent applications. The centralized illegal device manager periodically loads the list of illegal devices from the blacklist database and reports those events to the illegal device application, which generates new security rules to prevent the network traffic from/to those illegal devices.

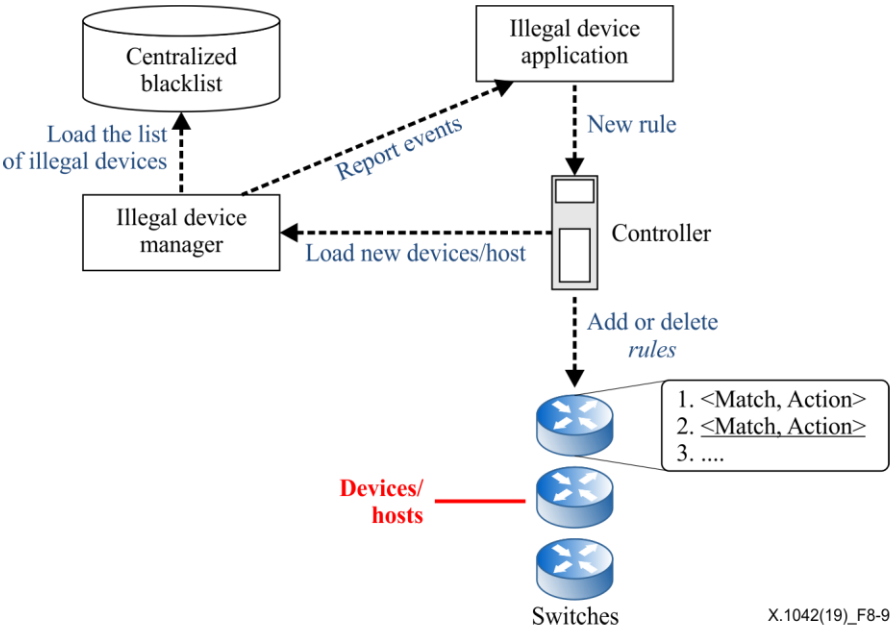


Figure 8-9 – Concept of a centralized illegal device management service

8.4.2 Service scenario of a centralized illegal device management service

Figure 8-10 shows an example scenario of a centralized illegal device management service to prevent traffic from a stolen mobile device.

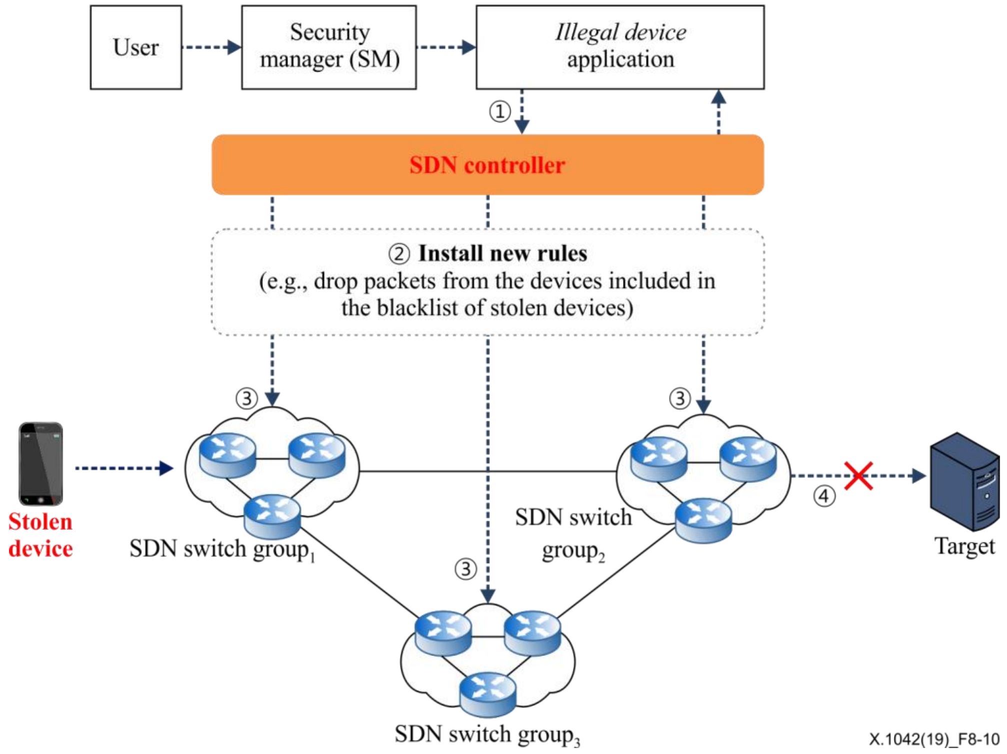


Figure 8-10 – Inter-domain scenario for a centralized illegal device management service

– Step 1. Illegal device management application installs new rules.

An illegal device application should specify a new rule when information about new stolen devices is reported by the centralized illegal device manager. As a precondition of this scenario, the illegal device application or SM adds the new rule (e.g., "Drop packets from those devices stored in a centralized blacklist of stolen devices") to the SDN controller.

– Step 2. An SDN controller distributes new rules.

A new rule might be distributed to each switch by an SDN controller after installing it. Therefore, the SDN controller sends a flow insert operation that contains the rule (e.g., "Drop packets from new stolen devices") to all SDN switches. It can also be managed centrally, so that a centralized illegal device manager or SM might determine security policies for their service through a single point, i.e., an SDN controller.

– Step 3. All SDN switches insert new rules into their flow tables.

All SDN switches add a flow entry dropping future packets from those devices to their flow tables when receiving the flow insert operation about stolen devices.

– Step 4. An SDN switch executes new rules.

An SDN switch completely drops packets when receiving packets from those devices. Any packets from those devices cannot be passed under applied rules. Thereafter, the execution result should be transmitted to the SDN controller.

NOTE – It is important that illegal devices be identified. A unique identity, assigned by the centralized illegal device manager, is used to identify an illegal device . If the SDN controller only identifies the network address, e.g., a device's Internet protocol (IP) address and media access control (MAC) address that can be dynamically changed, a new rule is installed and then the old one is deleted on the SDN controller each time the network address of an illegal device changes.

8.5 Access control management service

8.5.1 Basic concept of an access control management service

This clause describes the basic concept of an access control management (ACM) service. The ACM module with an SDN controller can manage access rights policies hierarchically. As shown in Figure 8-11, an ACM module manages access rights in order to prevent illegal access to resources.

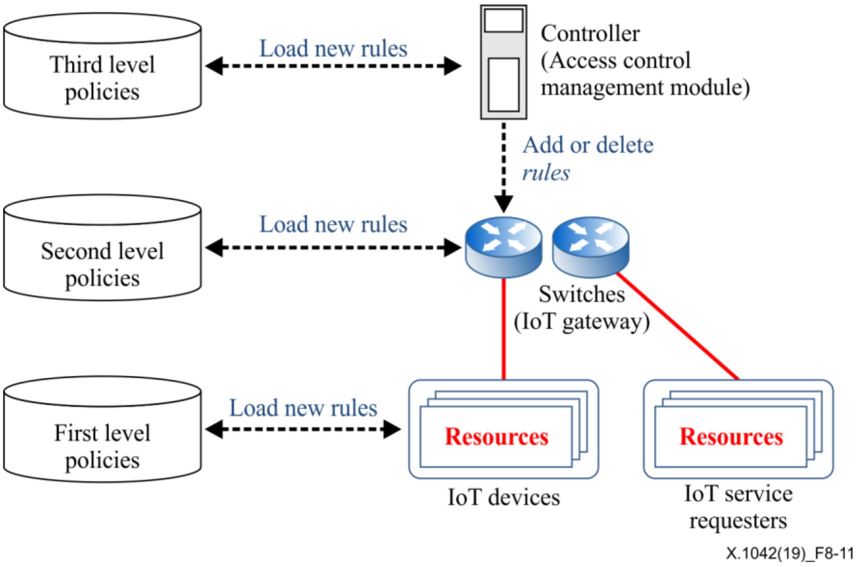


Figure 8-11 – Concept of access control management service

8.5.2 Service scenario of an access control management service

Figure 8-12 shows an example scenario of an ACM service managed by a security controller. This scenario involves both an SDN controller and switches.

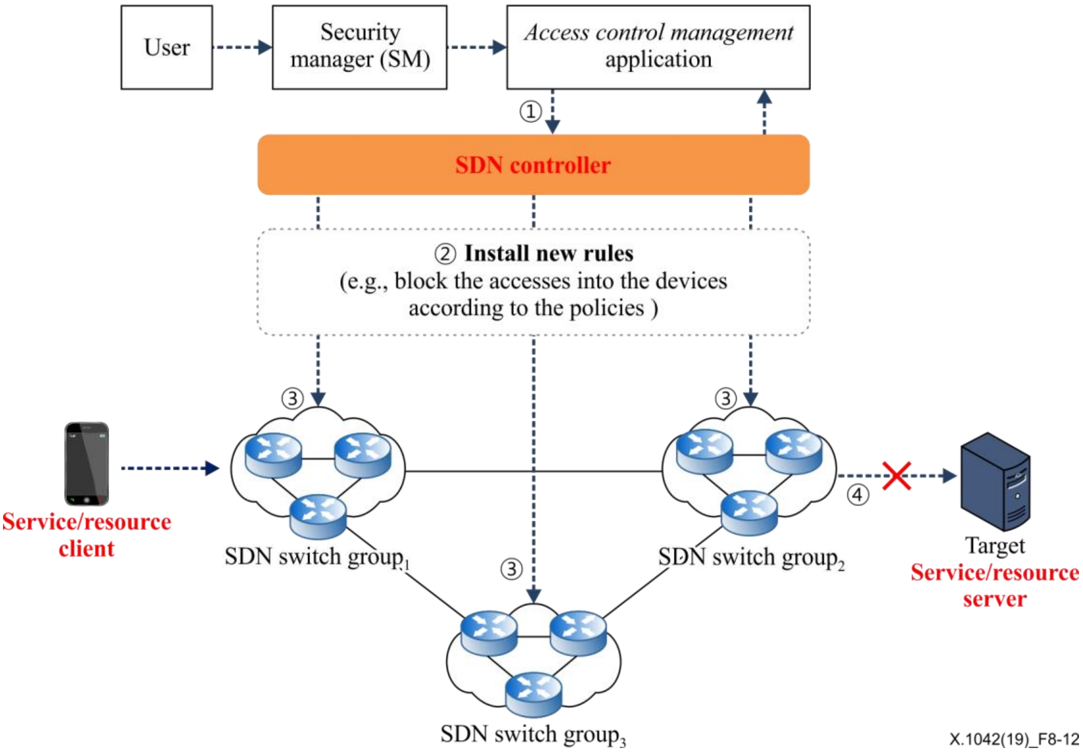

User
Security manager (SM)
Access control management application
①
SDN controller
② Install new rules (e.g., block the accesses into the devices according to the policies)
③
③
③
④
Service/resource client
SDN switch group$_1$
SDN switch group$_2$
SDN switch group$_3$
Target Service/resource server
X.1042(19)_F8-12

Figure 8-12 – Inter-domain scenario for an access control management service

– Step 1. An ACM application installs new policies from the SM.

An ACM application should specify new policies to access resources in distributed service/resource devices (e.g., IoT devices). As a precondition of this scenario, the SM has already added new policies to this ACM application.

– Step 2. An SDN controller distributes new rules.

A new rule or rules should be stored. Then they may be distributed to each switch by an SDN controller. The SDN controller may send an access request to operate the resource(s) to a service/resource device. In this case, an SDN controller does not receive any requests from SDN switches for rule distribution. The SDN switches may be able to ask the SDN controller to give access rules for resources in service/resource devices before sending requests for rule distribution to the SDN controller.

– Step 3. All SDN switches add new rules to their local database.

All SDN switches add new rules to their local database to process access authorization requests to service/resource devices.

– Step 4. An SDN switch executes new rules.

An SDN switch can completely drop packets when receiving packets from a service/resource client according to the access rules. Here, each SDN switch domain should be able to have different access rules according to the capabilities of each domain. Any packets from those clients cannot be passed via an SDN switch under applied rules. Any packets that do not have any access rules should be reported to the SDN controller for management by the ACM application.

Appendix I

Criteria for security services based on SDN

(This appendix does not form an integral part of this Recommendation.)

This appendix provides criteria for various security services.

I.1 Criteria for security services in intra-domain networks

I.1.1 Centralized firewall service

Legacy firewalls face challenges, e.g., their substantial cost, performance, management of access control, establishment of policy and packet-based access mechanisms. To address these challenges, this Recommendation presents the framework of a centralized firewall service based on SDN. Firewall rules can be managed flexibly by a centralized server. Existing SDN protocols can be used through standard interfaces between firewall applications and switches.

– Cost

The cost of adding firewalls to network resources, e.g., routers, gateways and switches, is substantial because firewalls need to be added to each network resource. To overcome this issue, each network resource can be managed centrally, so that a single firewall is manipulated by a centralized server.

– Performance

The performance of firewalls is often slower than the link speed of their network interfaces. Every network resource needs to check firewall rules without reference to network conditions. Firewalls can be adaptively deployed depending on network conditions in this framework.

– Management of access control

Since there may be hundreds of network resources in an administered network, the dynamic management of access control for security services like firewalls is a challenge. This is because firewall rules need to be dynamically added for new network attacks.

– Establishment of policy

Policy should be established for each network resource. However, it is difficult to describe which flows are permitted and denied within a specific organization network under management. Thus, a centralized view might be helpful to determine security policies for such a network.

– Packet-based access mechanism

A packet-based access mechanism is not enough in practice, since the basic unit of access control is usually users or applications. Therefore, application level rules need to be defined and added to the firewall service by an administrator.

I.1.2 Centralized honeypot service

Legacy honeypots have challenges, e.g., their substantial cost, performance, management of access control, establishment of policy and packet-based access mechanisms. To address these challenges, this Recommendation presents the framework of a centralized honeypot service based on SDN. Honeypot places can be managed flexibly by a centralized server. Existing SDN protocols can be used through standard interfaces between honeypot applications and switches.

– Cost

The cost of running additional honeypots in a network is substantial due to the need to use additional network resources, e.g., hosts for honeypots. To overcome this issue, honeypot places can be managed flexibly by a centralized server.

– Performance

The performance of honeypots depends on the capability of host machines. Every honeypot always runs in the same manner without reference to network or attack conditions. Honeypots can adaptively be deployed depending on network or attack conditions in this framework.

– Management of access control

Since there may be hundreds of network resources in an administered network, the dynamic configuration of honeypots is a challenge. This is because honeypot places need to be dynamically changed to defend against new attacks.

– Establishment of policy

Policy should be established for each network resource. However, it is difficult to determine specific honeypot places against suspicious attacks, depending on the network and attack conditions. Thus, a centralized view might be helpful to dynamically adjust security policies over time.

– Honeypot deployment mechanism

Honeypot places should be properly deployed depending on network and attack conditions. An SDN-based centralized honeypot service determines the optimal place to monitor and respond to attacks in real time. The honeypot is centrally configured as the intended attack target by a centralized server.

I.2 Criteria for security services in inter-domain networks

I.2.1 Centralized DDoS attack mitigation service

A centralized DDoS attack mitigation service defends servers against DDoS attacks outside private networks, i.e., from public networks. The servers are categorized into stateless servers (e.g., DNS servers) and stateful servers (e.g., web servers). Figure 8-6 shows the configuration of a DDoS attack mitigation service in a private network. Switches in the private network are configured in hierarchical domain levels: level-1 switches, level-2 switches, etc. Level-*n* switches for dynamic defence line up against a variety of DDoS attacks.

The centralized DDoS attack mitigation service faces challenges, e.g., the substantial cost, performance, management of access control, establishment of policy and packet-based access mechanisms. To address these challenges, this Recommendation presents the framework of a centralized DDoS attack mitigation service based on SDN. DDoS attack mitigation rules that can be managed flexibly by a centralized server. Existing SDN protocols can be used through standard interfaces between DDoS attack mitigation applications and switches.

– Cost

Each network resource can be managed centrally and flexibly with a minimum cost such that switches are configured and manipulated on multi-levels by a centralized server. As the severity of DDoS attacks for a server increases, multi-level switches perform selective drops of packets to reduce the impact of DDoS attacks. In other words, suspicious DDoS attack packets will be dropped earlier at the beginning of the routing path to the victim host.

– Performance

The performance of centralized DDoS attack mitigation is often slower than the link speed of its network interfaces. In the legacy service, every network resource needs to check DDoS attack mitigation rules without reference to network conditions. However, DDoS attack mitigation applications can adaptively be deployed depending on network conditions in this framework.

- Management of access control

  Since there may be hundreds of network resources in an administered network, the dynamic management of access control for security services like DDoS attack mitigation is a challenge. This is because DDoS attack mitigation rules need to be dynamically added for new DDoS attacks.

- Establishment of policy

  Policy should be established for each network resource. However, it is difficult to determine specific packet drop policies against DDoS attacks depending on network conditions. Thus, a centralized view might be helpful to dynamically adjust security policies over time.

- DDoS attack detection mechanism

  DDoS attack detection is performed by checking whether requests for services from a client come in an expected interval. The DDoS attack detection mechanism determines the probability that requests from a client are DDoS attacks and performs more frequent selective drops of the requests proportionally to the probability.

I.2.2 Centralized illegal device management service

Legacy illegal device management services have challenges, e.g., the substantial cost, performance, management of access control, establishment of policy and packet-based access mechanisms. To address these challenges, this Recommendation presents a centralized illegal device management service based on SDN. The rules for blacklisting devices can be managed globally. Existing SDN protocols can be used through standard interfaces between illegal device applications and switches.

- Cost

  The cost of updating blacklists for network resources, e.g., routers, gateways and switches, is substantial due to the need to update blacklists for each network resource individually. To overcome this issue, security rules related to blacklists for each network resource can be managed centrally, so that a single illegal device management service is manipulated by a centralized server.

- Performance

  Since packets from blacklisted devices are dropped at the beginning of the routing path, unlike the legacy management service, the performance of the centralized illegal device management service can be improved in practice.

- Management of access control

  When blacklists are locally managed, it is not easy to synchronize the locally distributed blacklists, since there may be hundreds of network resources in various countries. Security rules need to be dynamically added for new illegal devices.

- Establishment of policy

  Policy should be established for each network resource. However, it is difficult to describe what devices are disallowed within a specific organization network under management. Thus, a centralized view might be helpful to determine security policies for such a network.

- Blacklist update mechanism

  It is important to maintain an up-to-date blacklist of illegal devices. Therefore, existing legacy services must regularly update the blacklist database so as to retain the latest information on any illegal devices. In the centralized illegal device management service, the blacklist is centrally managed as a single logical database by a centralized server.

I.2.3 Access control management service

ACM services have challenges, e.g., the substantial cost, performance, management of access control, establishment of policy and packet-based access mechanisms. To address these challenges, this Recommendation presents an ACM service based on SDN. The rules for whitelisting devices can be globally managed in distributed network services (e.g., SDN controller, switch). Existing SDN protocols can be used through standard interfaces between ACM applications and switches through an SDN controller.

- Cost

  The cost of updating whitelists for network resources, e.g., routers, gateways and switches, is substantial due to the need to update whitelists for many network resources. To overcome this issue, the security policies related to whitelists of each network resource can be managed centrally, so that an ACM service can be manipulated by a centralized server.

- Performance

  Since packets from devices without access rights are dropped at the beginning of the routing path, unlike the legacy management service, the performance of the ACM service can be improved in practice. Additionally, information about access rights will be divided and stored in network resources according to their security level.

- Management of access control

  When whitelists are locally managed, they are not easy to synchronize, since there may be hundreds of network resources in various countries. Security rules need to be dynamically spread to transmit new access rights to network resources.

- Establishment of policy

  Policy should be established for each network resource according to its security level. However, it is difficult to describe which IoT devices are disallowed within a specific organization network under ACM. Thus, a centralized view might be helpful to determine security policies for such a network.

- Whitelist update mechanism

  It is really important to maintain an up-to-date whitelist of access rights for IoT devices. Therefore, existing legacy services must regularly update the whitelist database so as to retain the latest information on any access rights for IoT devices. In the ACM service, the whitelist is centrally managed as a single logical database by a centralized server. Additionally some parts of policies may be distributed into network resources.

Appendix II

An example of packet data scan detection

(This appendix does not form an integral part of this Recommendation.)

Packet data scan detection requires support in order to detect and mitigate against some attacks, e.g., worm files. The administrator configures the policies to randomly detect only some, not all, packets of the flow for higher performance. One possible schema for packet data scan detection [b-ICIN SDNSec] involves selection of the first *m* consecutive packets from each flow for packet data scan detection. This schema can be designed for all flows or for those only meeting certain conditions, e.g., packets from a certain source IP address or to a certain destination.

OpenFlow protocol [b-ONF TS-012], as one of the SDN southbound interface implementations, may be extended in order to support packet data scan detection. Two more additional features may be added into the format of the flow entry. These updates have to be reflected in both the controller and switches. One of these features is the schema that comprises packet data scan detection. The other feature is the condition which describes the flows that meets conditions configured by the administrator or applications. An optional action (OFPAT_DETECTION) should then be added in clause 5.12 of [b-ONF TS-012] as shown in the following text in italic: *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.* This new action is similar to the OFPAT_OUTPUT action in the OpenFlow protocol. Finally, action structures should be updated in clause 7.2.4 of [b-ONF TS-012] as shown in the following by text in italic.

```
    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);
```

Appendix III

Implementation architecture for security services based on SDN

(This appendix does not form an integral part of this Recommendation.)

III.1 Interface to the network security function framework with SDN in IETF

III.1.1 Overview

This clause provides an IETF interface to network security function (I2NSF) framework with SDN for cloud-based security services, e.g., firewalls, DPI and DDoS attack mitigation functions. SDN enables some packet filtering rules to be enforced in the network switches by controlling their packet forwarding rules. By taking advantage of this capability of SDN, it is possible to optimize the process of security service enforcement in the I2NSF framework.

Figure III.1 shows an I2NSF framework [b-IETF RFC 8329] with SDN networks to support network-based security services. In this framework, the enforcement of security policy rules is divided into SDN switches and network security functions (NSFs). Here, the NETCONF protocol and YANG modelling language are used.

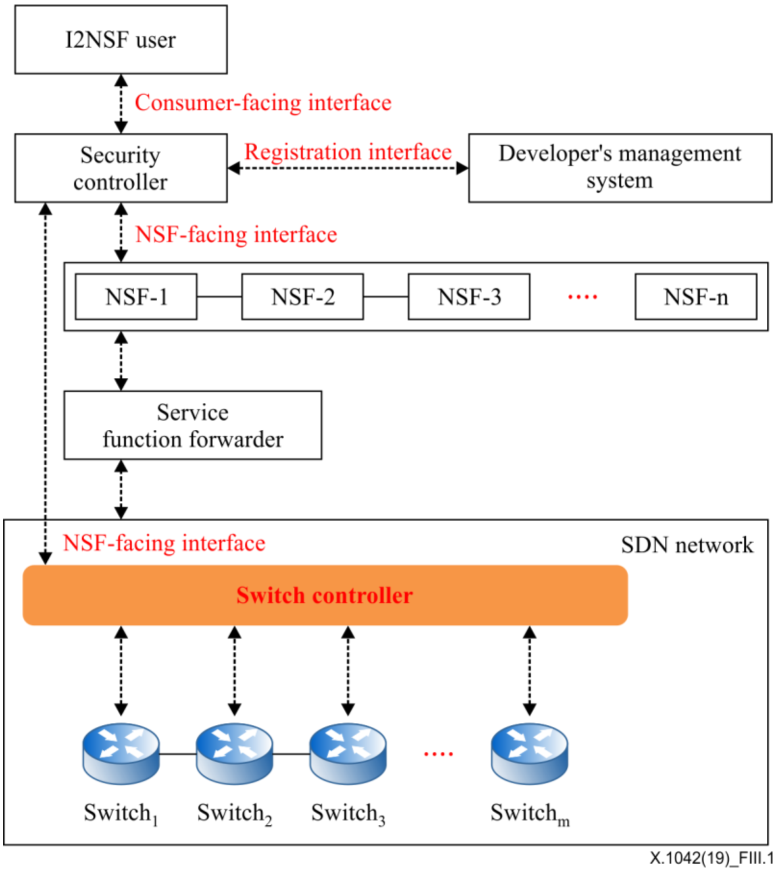


Figure III.1 – Interface to network security function framework in IETF

III.1.2 Comparison of IETF and ITU-T architectures

Figure III.2 illustrates the comparison of the I2NSF framework using SDN and ITU-T architecture. ITU-T components are shown in blue.

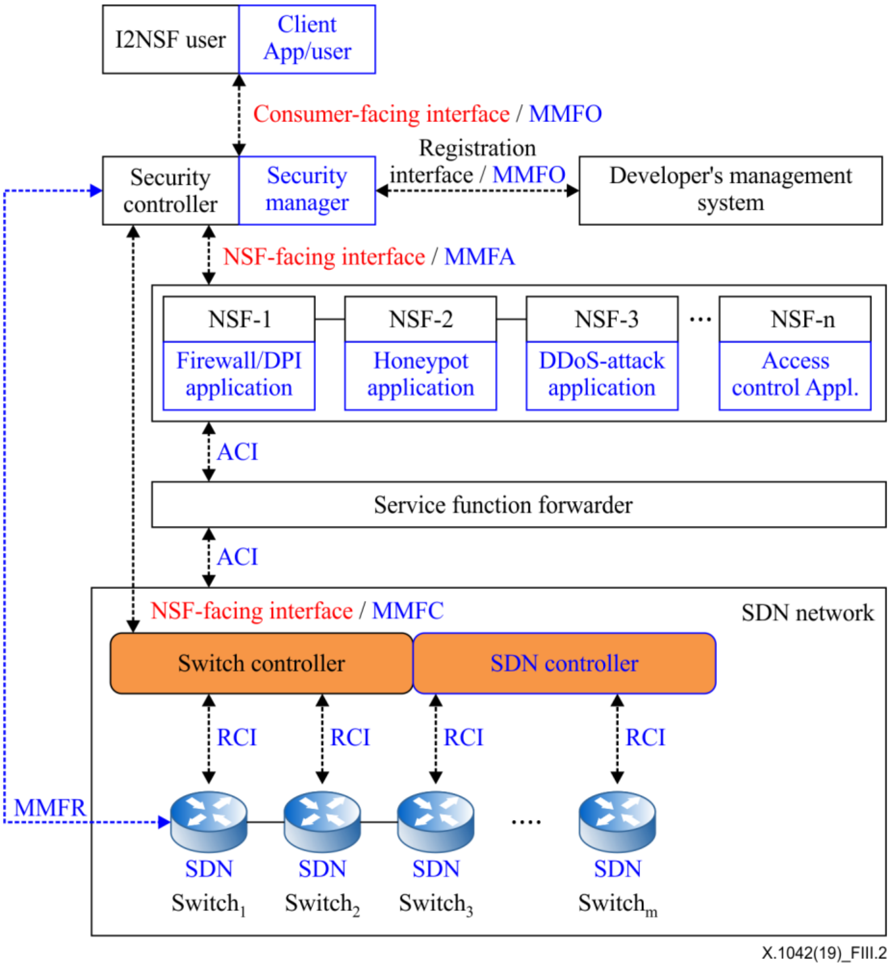


Figure III.2 – Comparison of IETF and ITU-T architectures

III.2 SDN architecture in the ONF

III.2.1 Overview

This clause provides the SDN architecture in the ONF. Figure III.3 shows the SDN architecture in [b-ONF TR-521]. In Figure III.3, SDN is modelled as a set of client-server relationships between SDN controllers and other entities that may themselves be SDN controllers. In its role as a server, an SDN controller may offer services to any number of clients, while an SDN controller acting as client may invoke services from any number of servers. As long as they exhibit appropriate interface behaviour, the internal details of entities that are not SDN controllers lie outside the scope of this architecture. Here, the OpenFlow protocol is used.

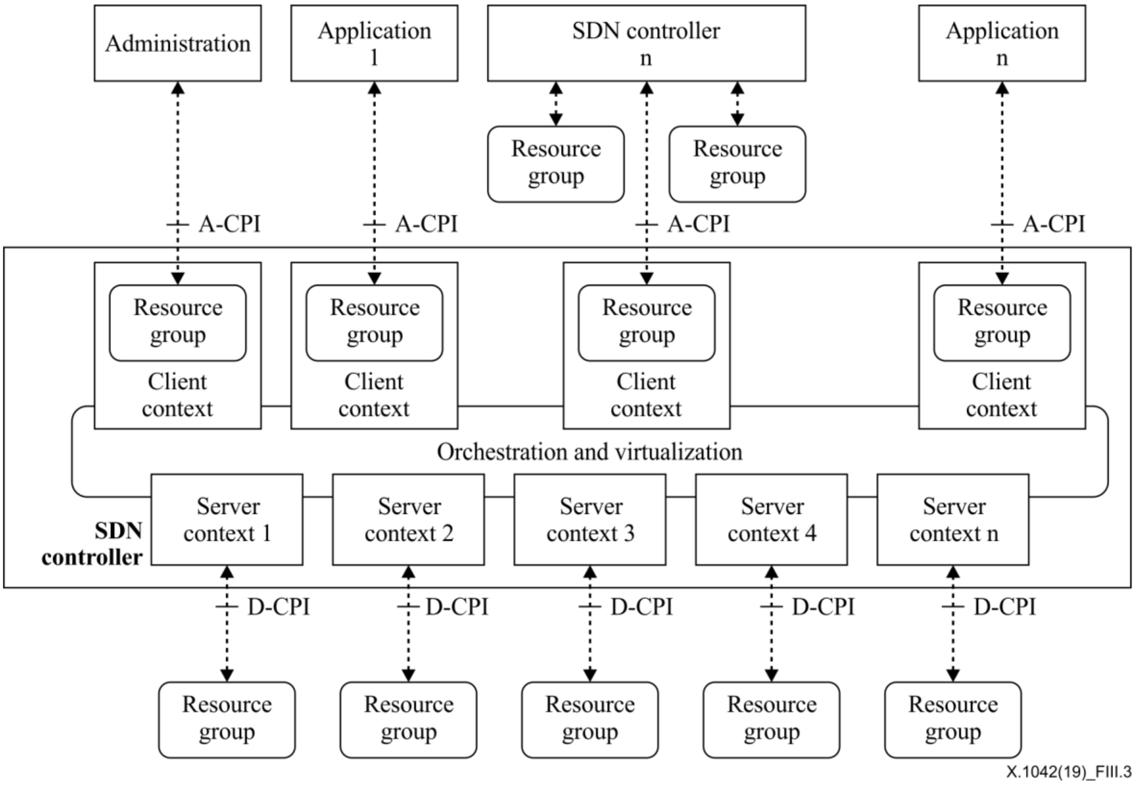


Figure III.3 – SDN Architecture in ONF

III.2.2 Comparison of ONF and ITU-T architectures

Figure III.4 illustrates the comparison of the ONF and ITU-T architecture. ITU-T components are shown in blue.

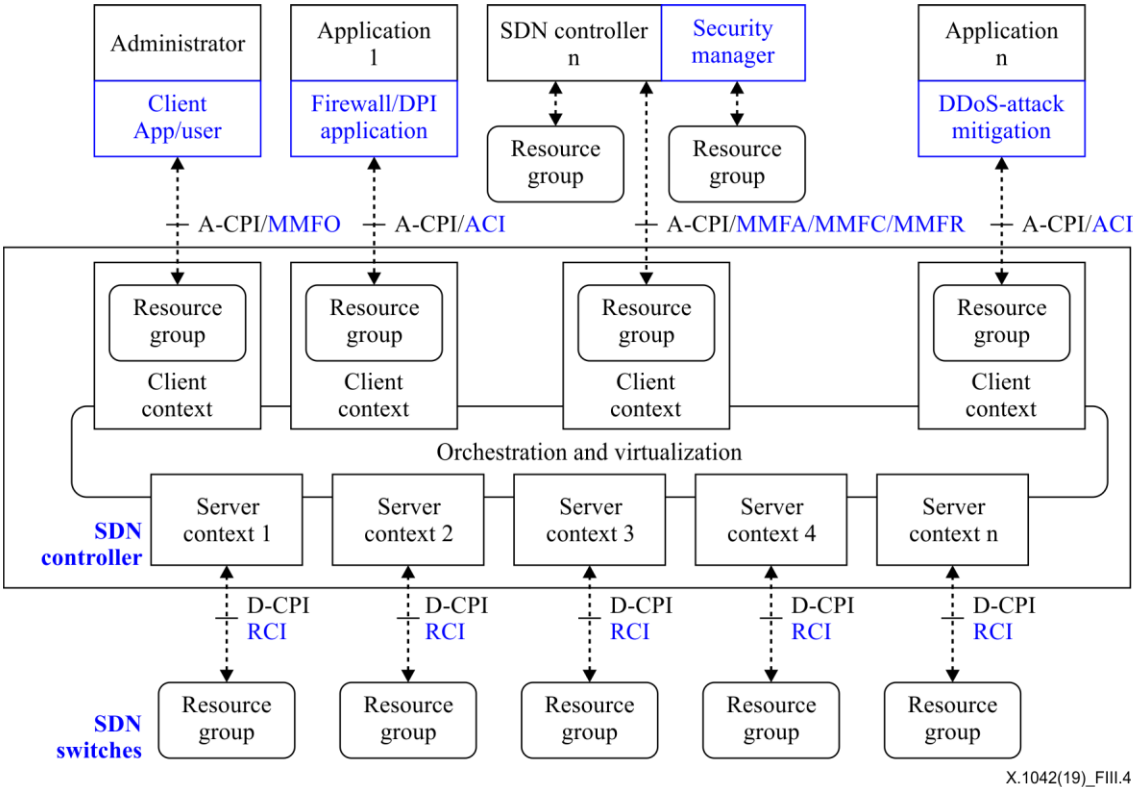


Figure III.4 – Comparison ONF and ITU-T architectures

Bibliography

[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

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019