International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1046

(12/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Network security

Framework of software-defined security in software-defined networks/network functions virtualization networks

Recommendation ITU-T X.1046

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
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
5G SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1046

Framework of software-defined security in software-defined networks/network functions virtualization networks

Summary

Recommendation ITU-T X.1046 specifies a framework of software-defined security in software-defined networks (SDNs) and the network functions virtualization (NFV) networks. This framework utilizes key advantages of SDN/NFV technologies such as on-demand capacity scale-in/scale-out, dynamic and intelligent security policy control regarding real-time network status, separated deployment of control layer and data forwarding layer, full view of traffic for monitoring and unified security policy setting.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1046	2020-12-14	17	11.1002/1000/14442

Keywords

SDN/NFV security, security controller, software-defined security.

* 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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Introduction

In recent years traditional telecommunication networks have shown their disadvantages such as long construction cycles, high costs and poor flexibility. These constraints are most evident in the slowdown on the development and deployment of emerging services.

The introduction of software-defined networks (SDNs) and network functions virtualization (NFV) technologies fundamentally changes the way networks are built and operated, mainly by taking advantage of general-purpose hardware, virtualization software and programmable services. With SDN and NFV, network operation and maintenance costs are reduced, resource utilization is improved, network flexibility is increased, and time-to-market of new services is considerably decreased.

SDN and NFV are considered as innovation technologies for telecommunications network evolution. However, these technologies bring new security challenges for telecommunications networks. Traditional security concepts based on static, passive, separate and manual operations of security defence systems do not work well in the SDN/NFV network environment. New security concepts based on dynamic, proactive, centralized and intelligent security management capabilities are needed.

This Recommendation provides a framework of software-defined security in SDN/NFV networks. This framework utilizes key advantages of SDN/NFV technologies such as on-demand capacity scale-in/scale-out, dynamic and intelligent security policy control regarding real-time network status, separated deployment of control layer and data forwarding layer, full view of traffic for monitoring and unified security policy setting. This framework is a layered framework, it provides security orchestration, centralized and automated security policy management, and intelligent security analysis and response.

Recommendation ITU-T X.1046

Framework of software-defined security in software-defined networks/network functions virtualization networks

1 Scope

This Recommendation specifies a framework of software-defined security in software-defined networks (SDNs) and the network functions virtualization (NFV) networks. This Recommendation provides the following:

– analysis of the main security challenges including technical and operational aspects in telecom operators' SDN/NFV based networks;

– summarization of security requirements to address these challenges in SDN/NFV networks;

– introduction of the concept of 'software-defined security' based on identified requirements;

– definition of a framework for 'software-defined security' with functionality requirements for each component; and

– guidelines on implementation of software-defined security.

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 X.1038] Recommendation ITU-T X.1038 (2016), *Security requirements and reference architecture for software-defined networking*.

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

[ITU-R M.1224-1] Recommendation ITU-R M.1224-1 (2012), *Vocabulary of terms for International Mobile Telecommunications (IMT)*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 security policy [ITU-R M.1224-1]: A set of rules which define and constrain the types of security-relevant activities of entities and parties.

3.1.2 policy conflict [b-ITU-T X.1036]: It defines the actions of two rules contradicting each other. The entity implementing the policy will not be able to determine which action to perform. To prevent this situation, the implementers of policy systems must provide conflict detection and avoidance or resolution mechanisms.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 distribution of security policy: A capability to distribute security policies to security functions.

3.2.2 flow collection function: A function for collecting network traffic so as to identify security threats. Commonly used technologies are those such as IP flow information export (IPFIX) [b-IETF RFC 3917] and sFlow [b-IETF RFC 3176].

3.2.3 forwarding policy: A set of rules which are distributed to switches by a SDN controller to indicate the way switches should forward network traffic.

3.2.4 lifecycle management of virtualized security function instance: A set of functions required to manage the instantiation, maintenance and termination of a virtualized security function.

3.2.5 network topology: Configuration of links connecting cross-connect physical devices (e.g., physical network device, physical security device) and virtualized functions such as virtualized network function (VNF) and virtualized security function (VSF).

3.2.6 optimization of security policy: Capabilities and operations to detect the activated security policies, redundant policies, usage frequencies, etc. and implement optimizations such as deleting non-activated security policies, merging or deleting redundant policies, etc.

3.2.7 security configuration parameter: A set of parameters which describe the features of the security function, such as maximum bandwidth, maximum number of connections, etc. supported by the security function, protected object and security actions of the security function.

3.2.8 security device: A physical device that provides security functions (e.g., firewalls, IDs, security gateways, and security management servers).

3.2.9 security information and event management system: A security and audit system that supports threat detection, compliance and security incident management through the analysis of security events.

NOTE – The security information and event management system collects, manages and analyses log events, and then produces operational advice or operates according to the results of the analysis.

3.2.10 security function vendor: A creator of a security function that provides physical/hardware security devices or software which executes security actions.

3.2.11 security function: Capabilities implemented in a physical/hardware device or by a software which executes security actions [b-UNISAFE] (e.g., detecting security malicious URLs, dropping a traffic, detecting DoS/DDoS attacks, scanning and removing viruses, traffic limit, access control based on source IP or destination IP, etc.) according to security policies.

3.2.12 security policy conflict: A contradiction when two security policies deal with the same flow, for example, one security policy is to drop a flow and another is to forward the flow.

3.2.13 service resource: A set of network devices in the telecom operator's network, which work together to deliver services to the telecom operator's customers.

3.2.14 security situation: Security information which is collected through continuous monitoring activities on a network in order to detect anomalies and potential security threats.

3.2.15 security situation awareness: Capability to provide information about the security situation.

3.2.16 SDN controller: A dedicated network element which provides a means to program, orchestrate, control and manage the network resources through software (i.e., SDN applications).

NOTE – Definition adapted from [ITU-T Y.3300].

3.2.17 software-defined security: Technologies enabling security capabilities such as decoupling of the security control plane with the enforcement plane of physical security devices, centralization of a decoupled security control plane, and opening of a programmable interface can achieve

uniformed identification of security functions, security function deployment on demand, collaborative work between security functions, automatic and on-demand distribution and configuration of security policies.

3.2.18 state of security function: A set of parameters that describe the supported resource state of the security function (e.g., central processing unit (CPU) capability, maximum bandwidth and throughput, etc.) and the usage state of the resources (e.g., CPU utilization, memory utilization, bandwidth utilization, etc.).

3.2.19 virtualized security function (VSF): A virtualized implementation of a security function that is deployed on a virtualization infrastructure such as an NFV virtualization infrastructure (NFVI).

3.2.20 virtualized security function instance: The run-time instantiation of the virtualized security function (VSF) software resulting from completing the instantiation of its components and of the connectivity between them, and using the virtualized network function (VNF) [b-ETSI NFV 003] deployment and operational information captured in the VNF descriptor of security function, as well as additional run-time instance-specific information and constraints.

3.2.21 virtualized security function scaling: An ability to dynamically extend/reduce resources granted to the virtual security function (VSF) as needed. This includes scaling up/down and scaling out/in. Scaling out/in is an ability to scale by add/remove VSF instances. Scaling up/down is an ability to scale by changing allocated resources of VSF, e.g., increase/decrease memory, central processing unit (CPU) capability or storage capacity.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
AV	Antivirus
C&C	Command and Control
CPE	Customer Premise Equipment
CPU	Central Processing Unit
DoS	Denial of Service
DDoS	Distributed Denial of Service
EMS	Element Management System
FW	Firewall
IP	Internet Protocol
IPS	Intrusion Prevention System
MANO	Management and Orchestration
NFV	Network Function Virtualization
NFVI	NFV Virtualization Infrastructure
NTQ	Network Topology Query
OAM	Operation, Administration and Maintenance
OSS	Operation Support System

RESTful	Representational State Transfer
SD-WAN	Software-Defined Wide Area Network
SDN	Software-Defined Network
SFR	Security Function Registry
SFSM	Security Function State Management
SIEM	Security Information and Event Management
SPCD	Security Policy Conflict Detection
SPDO	Security Policy Distributing and Optimizing
SPM	Security Policy Manager
SPMA	Security Policy Management
SPR&SFS	Security Policy Resolution and Security Function Selection
SPS	Security Policy Repository
TLS	Transport Layer Security
URL	Uniform Resource Locator
vIPS	Virtual Intrusion Prevention System
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNF	Virtualized Network Function
VNFC	VNF Component
VNFM	VNF Manager
VPN	Virtual Private Network
VSF	Virtualized Security Function
VSRM	Virtualized Security Resource Management
WAN	Wide Area Network

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 keyword "operator" indicates telecom operator.

Italics are used in this Recommendation to indicate components of security manager and security analyser.

Bold fonts are used in this Recommendation to indicate layers in the framework of software-defined security in software-defined networks/network functions virtualization networks.

6 Overview

In recent years traditional telecommunications networks have revealed disadvantages such as long construction cycles, high costs and poor flexibility. These constraints are most evident in the slowdown on the development and deployment of emerging services. The introduction of software defined networks (SDNs) and network functions virtualization (NFV) technologies fundamentally changes the way networks are built and operated, mainly by taking advantage of general purpose hardware, virtualization software and programmable services. With NFV providing automatic on-demand virtualized resource management and SDN offering automatic routing together with finer granularity of policies on network configuration and data flow scheduling, network operation and maintenance costs are reduced, resource utilization is improved, network flexibility is increased and time-to-market for new services is considerably decreased.

These changes also affect the security of these new telecommunications networks. Traditional static, passive, separate and manual operations of security defence systems do not work well in new cloud-based SDN/NFV networks. A new security system architecture is needed to meet the urgent requirement of dynamic, proactive and intelligent security management within SDN/NFV networks.

7 Security challenges for SDN/NFV network

SDN and NFV are considered innovative technologies driving the evolution of telecommunication networks. They improve network flexibility and reduce deployment and operation costs. However new security challenges are also introduced and should be addressed. These security challenges are divided into two aspects: (1) security challenges of SDN and NFV, and (2) management and operation challenges to security policy and security devices. These security challenges are described in detail as follows:

(1) Security challenges of SDN and NFV:

- spoofing and DoS attacks for SDN controller [ITU-T X.1038];
- flow rules confliction on SDN controller [ITU-T X.1038];
- loss of confidentiality and integrity in NFV [b-ETSI NFV-SEC 003].

[ITU-T X.1038] specified security requirements and reference architecture for SDN. The security requirements of NFV were defined by the ETSI specification [b-ETSI NFV-SEC 003]. Therefore, the security requirements of SDN and NFV will not be included in this Recommendation.

(2) Management and operation challenges to security policy and security functions:

- the physical security boundary becomes blurred after introducing virtualization. This means traditional protection methods, which depend on deploying security devices and setting security policies at physical boundaries, cannot meet the protection requirements of virtualized boundaries;
- various kinds of security devices lead to complicated security management and operation issues. Security devices from different security device vendors have different configuration and operation mechanisms. This increases administrator workloads and may result in misconfiguration;
- scalability of security devices is difficult and costly. The scaling of traditional security devices (such as traditional telecommunication network devices) requires procedures for purchase, deployment and operations. These procedures impose long-term and costly impacts;
- single point protection of security devices leads to limited protection capabilities within the operators' networks. SDN and NFV result in new security challenges for operators' networks. For example, virtualization results in invisible communications between two VNFs that are running on the same host. Attacks between these two VNFs cannot be identified by traditional security detection methods. Thus, the passive defence of a

single point security device cannot identify new types of attacks, advanced persistent threats (APTs), etc., introduced by VNFs;

– dynamic VNF creation and deletion lead to complicated security management and operation issues. Traditional operators' networks utilize security devices deployed in specific locations (i.e., physical boundaries) that are operated manually. Therefore, it may be impossible to deploy security policies sufficiently quickly and correctly when VNFs are used. This may result in attacks for VNFs, e.g., an attacker targets a VNF which has not loaded the proper security protection mechanism.

8 Requirements for software-defined security in SDN/NFV networks

To address the security challenges to management of security policies and security functions as identified in (2) in clause 7, in SDN/NFV networks, security requirements related to management of security policies and security functions in SDN/NFV networks are defined as follows:

1) it is recommended that security functions and security policies are deployed on demand;
2) it is recommended that security functions are uniformly identified and managed;
3) it is recommended to offer virtualized security functions in order to enable fast deployment, efficient operation and cost reduction;
4) it is recommended that security functions collaboratively work together to proactively defend against security threats;
5) it is recommended that security policies are generated quickly and automatically distributed and configured.

To meet the above security requirements, the concept of software-defined security is proposed in this Recommendation. Software-defined security is based on SDN/NFV technologies and has the capabilities of decoupling the control plane with the enforcement plane of physical security devices, centralization of the decoupled control plane and an open programmable interface, which can realize deployment and scaling of a security function on-demand, centralized managing and configuring of a security function and security policy, etc.

Clause 9 proposes the reference framework of software-defined security with related components and interfaces. The **security managed control and analysis layer** in the framework of software-defined security centrally manages the security functions and security policies, deploys the security functions and security policies according to the security configuration parameters of the **security service laye**r. It coordinates the work among the security functions to realize proactively. The virtualized security functions of the s**ecurity enforcement layer** can be scaled on demand through cooperation between the **security managed control and analysis layer** and NFV MANO [b-ETSI NFV 003]/SDN controller [ITU-T Y.3300].

Clause 10 proposes two implementations of software-defined security so as to guide the deployment of the software-defined security framework.

9 Reference framework of software-defined security

9.1 Reference framework

Considering the benefits of SDN and NFV, physical security devices and virtualized security functionalities can be offered to support on-demand, quick deployment and implementation, as well as flexible scaling. Furthermore, decoupling the control plane with the enforcement plane of physical security devices and centralization of the decoupled control plane can achieve uniform identification of security functions, collaborative work between security functions, and automatic and on-demand distribution and configuration of security policies. Figure 1 illustrates a reference framework of software-defined security.

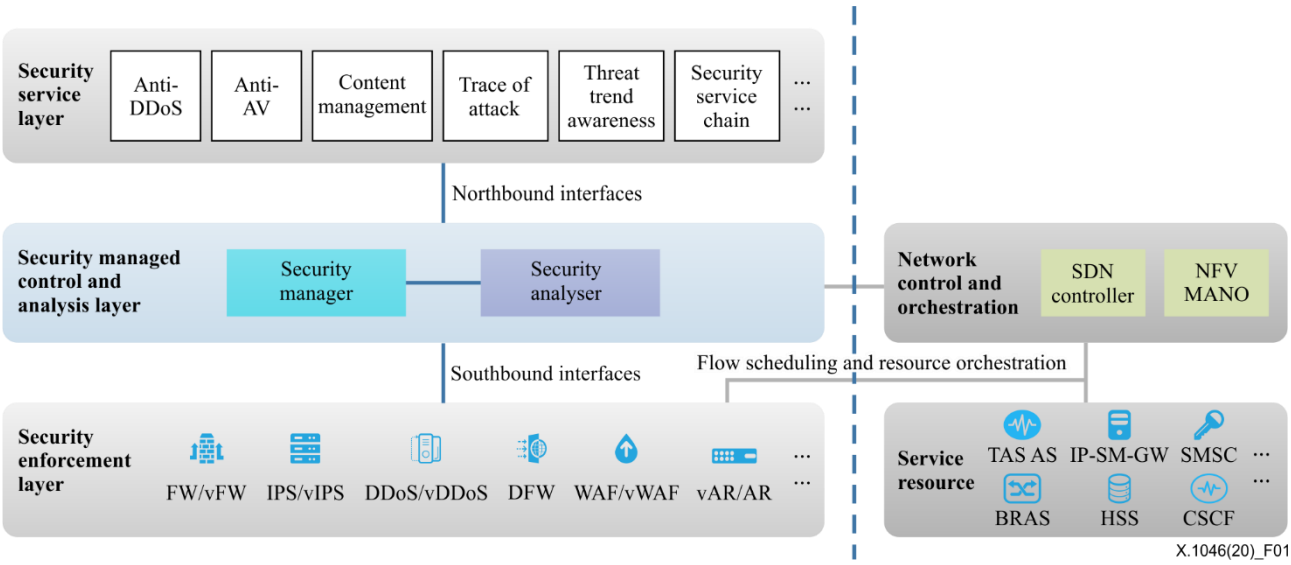

Figure 1 – Reference framework of software-defined security

The reference framework of software-defined security includes three layers and two interfaces:

– **Security service layer**: This layer describes security services provided by telecom operators, e.g., anti-distributed denial of service (DDoS), antivirus (AV), security service chain, etc. A request from a customer for a security service that includes its related security configuration parameters (e.g., required network bandwidth, protected source and destination IP addresses), is sent to the **security managed control and analysis layer** through the northbound interface.

– **Security managed control and analysis layer**: This layer sits in the centre of this reference framework of software-defined security. It includes a security manager and a security analyser.

– The security manager manages security functions according to the security configuration parameters, which are generated from the **security service layer** or the security analyser. The security manager maps the received security configuration parameters to security policies. The security manager also collaborates with the SDN controller [ITU-T Y.3300], NFV management and orchestration (MANO) [b-ETSI NFV 003] to achieve flow scheduling and security resources orchestration [ITU-T Y.3300], [b-ETSI NFV IFA 010].

– The security analyser sends security configuration parameters to the security manager after analysing security logs and flows. The security logs and flows are gathered from security functions in the **security enforcement layer** and from network devices in 'service resource' respectively. The security analyser also provides security data such as threat trend awareness to the **security service layer**.

– **Security enforcement layer**: This layer describes virtualized security functions (VSF) and physical security devices which enforce security policy for flows and packages. These security policies are sent by the **security managed control and analysis layer**. NFV MANO [b-ETSI NFV 003] orchestrates and manages the virtualized resource and lifecycle of a virtualized security function, e.g., providing CPU resources for the virtualized security function, creating a new virtualized security function, etc.

– Northbound interfaces: This is the interface between the **security service layer** and the **security managed control and analysis layer**.

– Southbound interfaces: This is the interface between the **security managed control and analysis layer** and the **security enforcement layer**.

Detailed descriptions of the components and the interfaces of the reference framework of software-defined security are described in the following clauses.

9.2 Components

9.2.1 Security manager

The security manager is responsible for management of security functions and security policies according to received security configuration parameters from the **security service layer** and /or the security analyser. Figure 2 describes the components which are included in the security manager.

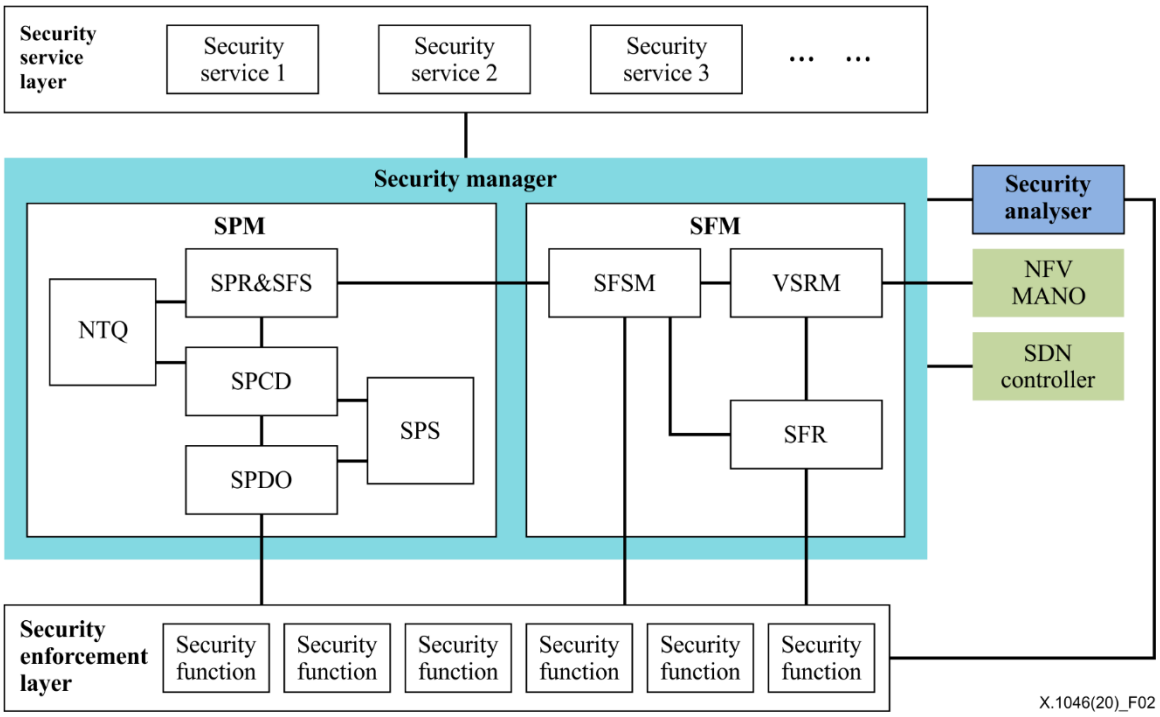

Figure 2 – Components in security manager

The security manager includes the *security policy manager (SPM)* component and the *security function manager (SFM)* component which are composed by some sub-components.

Security policy manager (SPM)

The *security policy manager* includes: the *security policy resolution and security function selection (SPR&SFS)* component, the *security policy conflict detection (SPCD)* component, the *security policy distributing and optimizing (SPDO)* component, the *network topology query (NTQ)* component, and the *security policy repository (SPS)* component. The capabilities of each component are described as follows:

– *Security policy resolution and security function selection (SPR&SFS)*: After receiving security configuration parameters from the **security service layer** or the security analyser, *SPR&SFS* is responsible for mapping the received security configuration parameters to security policies. Then *SPR&SFS* selects security function(s) according to the security policies.

– When a security configuration parameter from the **security service layer** or the security analyser is received, the *SPR&SFS* maps the received security configuration parameter to the appropriate security policy, resolves the security policy which includes the requested security function(s), protected network segment, IP address(es), and traffic handling policy, etc. Then, the *SPR&SFS* queries the state of the security function(s) which related the requested security function(s) from the *security function state management (SFSM)*, and queries the network topology from the *NTQ*. The queried security function states are combined with the queried network topology, the *SPR&SFS* selects the security function according to the security policy. If the required security function cannot be found (e.g., the

running security functions according to the security policy are busy and cannot be used, or there is no required security function in all running security functions), the *SPR&SFS* will initiate a process to create a new required security function instance. In the end, the selected security function instance identifier(s) and the resolved security policy are sent to the *SPCD* component.

– *Security policy conflict detection (SPCD)*: it is responsible for checking whether there is a security policy conflict. After receiving the security function identifier(s) and related security policy, the *SPCD* queries the *security policy repository (SPS)* and combines the network topology which queried from the *NTQ* to check whether there is a security policy conflict. If there is no security policy conflict, the security function identifier(s) and the related security policy are sent to the *SPDO* by the *SPCD*. The security policy is also sent to the *SPS* for storage. Otherwise, the *SPCD* handles the conflicted security policy according to the priority of the security policy or sends an alarm to the administrator.

– *Security policy distributing and optimizing (SPDO)*: it is responsible for distributing the security policy to the related security function(s) and optimizing the security policies on the security function(s). After receiving the security function identifier(s) and related security policy, the *SPDO* distributes the security policy to the related security functions. The *SPDO* periodically collects the states of the security policies on the security functions to detect the activated security policies, redundant policies, usage frequencies, etc. and optimizes the security policies. The optimized security policies are simulated to evaluate the impact to the service. After successful simulation, the optimized security policies are sent to the security function(s) and the *SPS* respectively, by the *SPDO*.

– *Network topology query (NTQ)*: it is responsible for querying the network topology through the northbound interface of the SDN controller [ITU-T Y.3300]. The query request can be sent periodically by the *SPR&SFS* and the *SPCD* to the *NTQ*. The network topology information is also sent to the *SPR&SFS* and the *SPCD* by the *NTQ*, after changing the network topology.

– *Security policy repository (SPS)*: it is responsible for storing the security policies and responding the security policy query requests from the *SPR&SFS* and the *SPCD*. The security policy on a security function is stored with the security function identifier.

Security function manager (SFM)

The *security function manager* includes: the *security function registry (SFR)* component, the *security function state management (SFSM)* component, and the *virtualized security resource management (VSRM)* component. The capabilities of each component are described as follows:

– *Security function registry (SFR)*: it is responsible for registering the security function. The security function registry information includes security function identifier, version, security function vendor identifier, throughput, bandwidth, CPU, memory, I/O capability, etc. A security function can be registered using the interface between the *SFR* and the security function. The security function provides support to proactively send its registry information to the *SFR* and also provides support to passively send its registry information after receiving the security function registry query request from the *SFR*. The vendor which provides the security function also supports the transformation of the security functions to *SFR* through secure channels to complete security function registration.

– *Security function state management (SFSM)*: it is responsible for managing the state of the security function. The dynamic states of a security function such as CPU utilization, memory utilization, bandwidth utilization, concurrency, etc. are periodically sent to the *SFSM* by the security function, and are queried by the *SFSM*. The static states of a security function such as CPU, memory, maximum bandwidth, throughput, etc. are queried from the *SFR* by the *SFSM*. The *SFSM* provides security function states to the *SPR&SFS* and the *VSRM*.

– *Virtualized security resource management (VSRM)*: it is responsible for requesting virtualized security function scaling to NFV MANO according to the virtualized security function state or request from the *SPR&SFS*. After successfully scaling or creating a virtualized security function, the scaled virtualized security function is registered to the *SFR*.

9.2.2 Security analyser

The security analyser is responsible for analysing the collected security logs from the security functions, and the gathered network flows from the service resource. After detecting the attacks, the security analyser provides security policies to the security manager. Figure 3 describes the components in the security analyser.

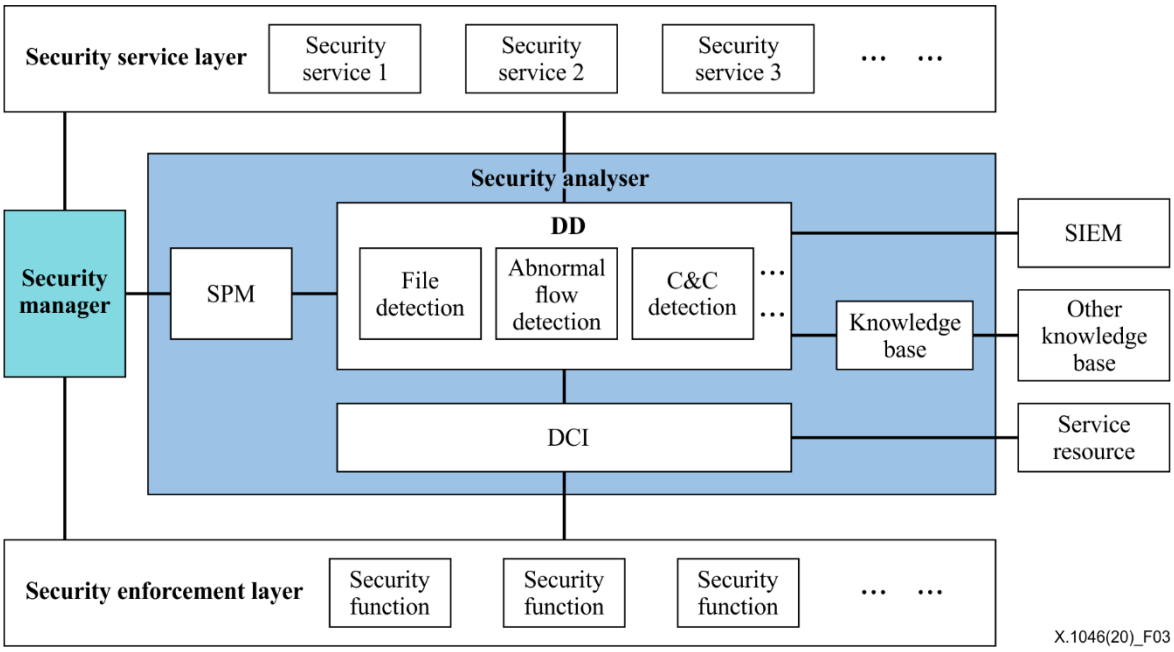

Figure 3 – Components in security analyser

The security analyser includes the data collection and initialization (DCI) component, data detection (DD) component, security policy management (SPMA) component, and knowledge base component. The capabilities of each component are described as follows:

– *Data collection and initialization (DCI)*: it is responsible for collecting and initializing the security logs on the security functions and the flows from the network devices in the service resource. The security logs and flows are actively sent to the *DCI* by the security functions and the flow collection functions respectively. The flow collection functions could be deployed in the physical switch or deployed as a standalone application. The *DCI* also periodically supports the query the security function and flow collection functions to get the security logs and the network flows respectively. The collected data may be raw network flows containing amounts of unnecessary information. The *DCI* is responsible for the initialization of the collected data, which means to extract useful information (such as security events, application protocols, related metadata, etc.) from the raw network flow. The initialized data is actively or passively sent to the *DD*.

– *Data detection (DD)*: it is responsible for detecting attacks according to the received initialized data from the *DCI*. Some detection engines such as file detection, abnormal flow detection, C&C detection, etc. are included in this component. Big data analysis and AI are utilized to deeply detect attacks by these detection engines. The *DD* supports the analysis of the data from other systems, e.g., security information and event management (SIEM). The

detection result is sent to the *SPMA*. The result could also be sent to the security situation awareness service.

– *Security policy management (SPMA)*: it is responsible for generating the security configuration parameters according to the detection result from the *DD* and sending the security configuration parameters to the security manager.

– *Knowledge base*: it is responsible for storing the malicious code and virus characteristics, malicious IP/URL/domain name, attack event, etc., which are referred by the *DD*. The *DD* also has capability to store the detected malicious code and virus characteristics, etc.

9.2.3 Security function

Security functions are included in the **security enforcement layer**. It is a physical or virtualized security function. After receiving the security policy from the security manager, the security function is responsible for handling flows according to the received security policies, e.g., forwarding flows, dropping flows, etc. The security functions are recommended to have the following capabilities:

– To actively register themselves to the security manager and passively send their registration information to the security manager after receiving the request message 'security function registry query'.

– To actively send their state to the security manager and passively send their state to the security manager after receiving the request message 'security function state query'.

– To actively send their security policies state to the security manager and passively send the security policies state to the security manager after receiving the request message 'security policy state query'.

– To scale up/down and scale out/in as described in clause 3.2.21, which is controlled by NFV MANO [b-ETSI NFV 003].

9.3 Interfaces

9.3.1 Northbound interfaces

The northbound interfaces are responsible for sending security configuration parameters according to the customer's security service request to the security manager. The security situation from the security analyser is also sent via northbound interfaces to a security situation awareness application. Northbound interfaces could support representational state transfer (RESTful) [b-RESTful] connections which could use transport layer security (TLS) [b-IETF RFC 5246] to protect these communications.

9.3.2 Southbound interfaces

The southbound interfaces are responsible for sending security policies to the **security enforcement layer** from the **security managed control and analysis layer**. The security log, registration information and state of the security functions from the **security enforcement layer** to the **security managed control and analysis layer** are also sent through the southbound interfaces. It is recommended to use TLS to protect the communications. The following interfaces are included at least:

– Security policy control interface: This interface is responsible for distributing the security policies from the security manager and collecting security policies from the security functions.

– Security function management interface: This interface is responsible for transmitting the registration information, state and security logs of the *security function instances* to the security manager and the security analyser respectively.

Figure 4 shows an overview of the northbound and southbound interfaces.

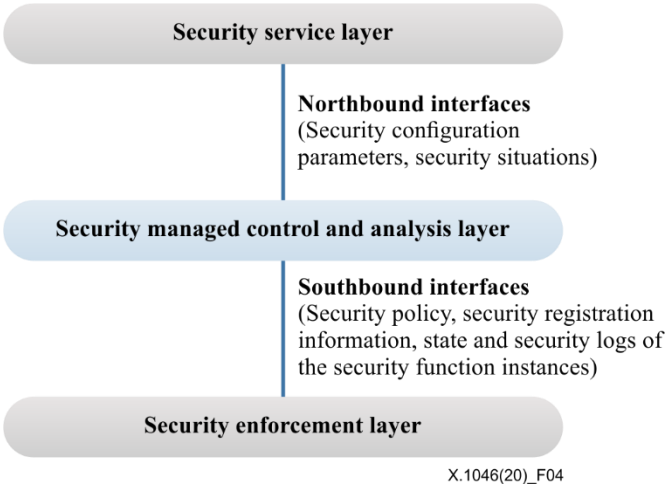

Figure 4 – Overview of the northbound and southbound interfaces

9.3.3 Interface details

For further details on northbound and southbound interface implementations, refer to [b-IETF RFC 8329], [b-OASIS OpenC2-L], [b-OASIS OpenC2-H] and [b-OASIS OpenC2-P].

9.4 Lifecycle management of virtualized security function instance

9.4.1 Creation of new security function instance

The *security manager* will create a new security function instance when it receives a security policy from the **security service layer** or the security analyser when there is no available security function according to the security policy (e.g., there is no required security function in all of the running security functions). Figure 5 describes the detailed procedures of creating a new security function instance.

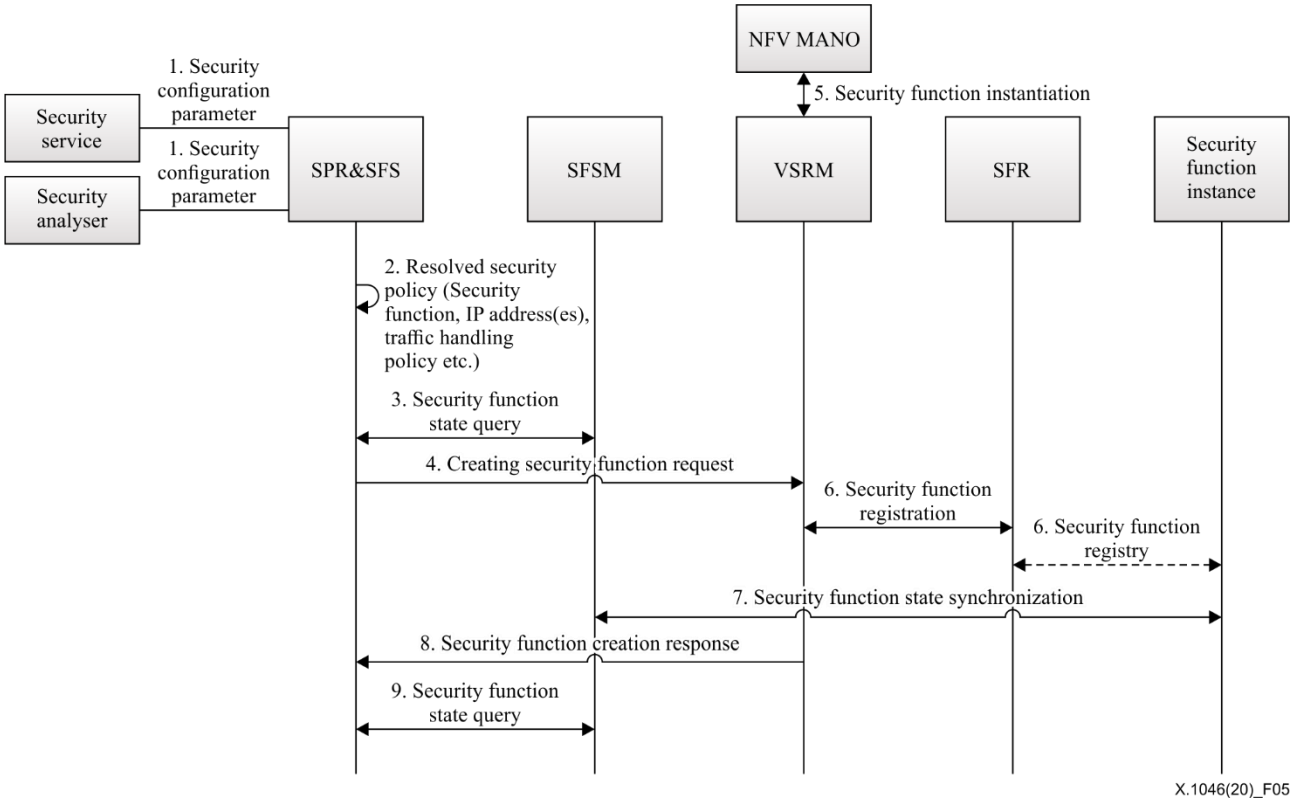

Figure 5 – Creation of a new security function instance

The procedures of creating a new security function instance described in Figure 5 are as follows:

1) The *SPR&SFS* receives a security configuration parameter from a security service in the **security service layer** or the security analyser.
2) The *SPR&SFS* maps the received security configuration parameter to an appropriate security policy and then resolves the security policy.
3) The *SPR&SFS* queries the security function state from the *SFSM* component, and finds that there is no available security function according to the extracted security function.
4) The *SPR&SFS* requests the *VSRM* to create the requested security function instance.
5) The *VSRM* requests NFV MANO to instantiate the requested security function.
6) The *VSRM* registers the *security function* (i.e., the instantiated security function) to the *SFR*. The security function instance could also register itself.
7) The security function state is synchronized between the *SPR* and the *SFS*.
8) The *VSRM* sends the security function creation response to the *SPR&SFS*.
9) The *SPR&SFS* sends the security function state query to the *SFSM* after receiving the security function creation response. Then, this component selects the security function instance, and the initial configuration of the security function instance will be implemented (see Figure 7).

9.4.2 Deletion of security function instance

A security function instance will be deleted when the *VSRM* finds the security function instance is activated but does not provide security service (such as filtering traffic, detecting abnormal traffic, etc.) for a period of time. Figure 6 describes the detailed process of deleting a security function instance.

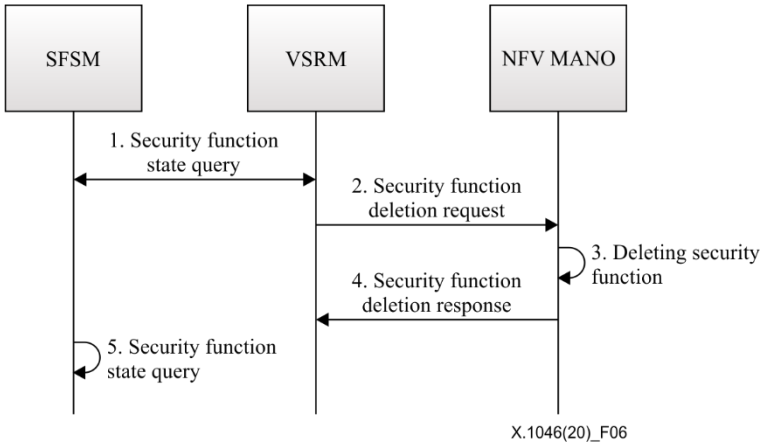

Figure 6 – Deletion of a security function instance

The deletion of a security function instance, as shown in Figure 6, includes the following steps:

1) The *VSRM* periodically queries the security function state.
2) The *VSRM* sends security function deletion request to NFV MANO when it finds that there is a security function instance but does not provide security service for a period of time. This security function deletion request includes the security function instance identifier, IP address, VLAN ID, etc.
3) NFV MANO deletes the security function instance according to the received request.
4) NFV MANO sends security function deletion response to the *VSRM* to indicate that the security function instance has been deleted.

5) The *SFSM* queries the states of the security function instance in the security enforcement layer and updates the stored states of the security function instance.

9.4.3 Configuration of security function instance

9.4.3.1 Initial configuration of security function instance

When a new security function instance is created according to the procedures shown in Figure 4, the security manager implements the initial configuration of the security function instance according to the security policy of the security service or the security analyser. Figure 7 describes the detailed procedures of initial configuration for the security function instance.

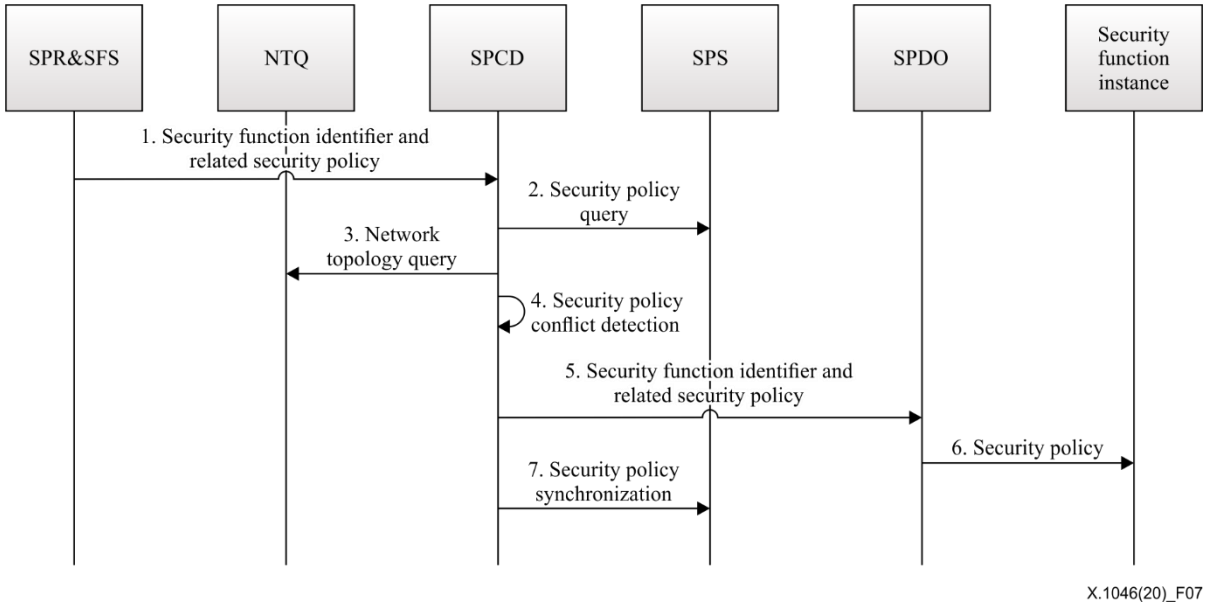

Figure 7 – Initial configuration of a security function instance

The procedures of initial configuration of a security function instance, as shown in Figure 7, include the following steps:

1) When a new security function instance is created, the *SPR&SFS* sends the selected security function identifier and related security policy to the *SPCD*.

2) The *SPCD* queries the stored security policy in the *SPS*.

3) The *SPCD* queries the network topology from the *NTQ*.

4) According to the network topology, the *SPCD* uses the security policy conflict detection algorithm to detect the conflict between the received security policy and the stored security policy. If there is no security policy conflict, step 5 will be implemented. Otherwise, the *SPCD* deals with the security policy conflict, such as selecting a security policy according to the priority of the security policy or issuing an alarm to the operation, administration and maintenance (OAM) process.

5) The *SPCD* sends the security function identifier and related security policy to the *SPDO*.

6) The *SPDO* configures the identified security function instance according to the security policy.

7) The *SPCD* synchronizes the security policy to the *SPS*.

9.4.3.2 Deletion of a security function instance configuration

Deleting a configuration of a security function instance can be implemented in the following two scenarios:

1) A customer who purchases a security service in the **security service layer** or the security analyser could decide to delete an existing configuration of a security function instance. Deleting the existing configuration of a security function instance will be implemented like the initial configuration of a security function instance in Figure 7. The priority of the security policy which is resolved from the deleting of the existing configuration of the security function instance is required to be set higher, then the security policy will be implemented by the security function instance.

2) The *SPDO* decides to delete a configuration of a security function instance, e.g., this configuration is redundant or out of date and will not be used.

9.4.3.3 Update of a security function instance configuration

Updating of the configuration of a security function instance can be implemented in the following two scenarios:

1) Like the configuration deletion of a security function instance, the configuration update of a security function instance can also be implemented like the initial configuration of a security function instance in Figure 7. The priority of the security policy which is resolved from the updating configuration of the security function instance is required to be set higher, and then the security policy will be implemented by the security function instance.

2) The *SPDO* decides to update an existing configuration of a security function instance, e.g., the configuration is out of date.

10 Reference implementation of software-defined security

10.1 Software-defined security deployment in NFV environment

The deployment of a software-defined security framework in an NFV environment improves the efficiency of the security detection and disposal in the NFV network, as well as the efficiency of the operation and maintenance for the security functions. Figure 8 proposes an example of the deployment of software-defined security in NFV environment.

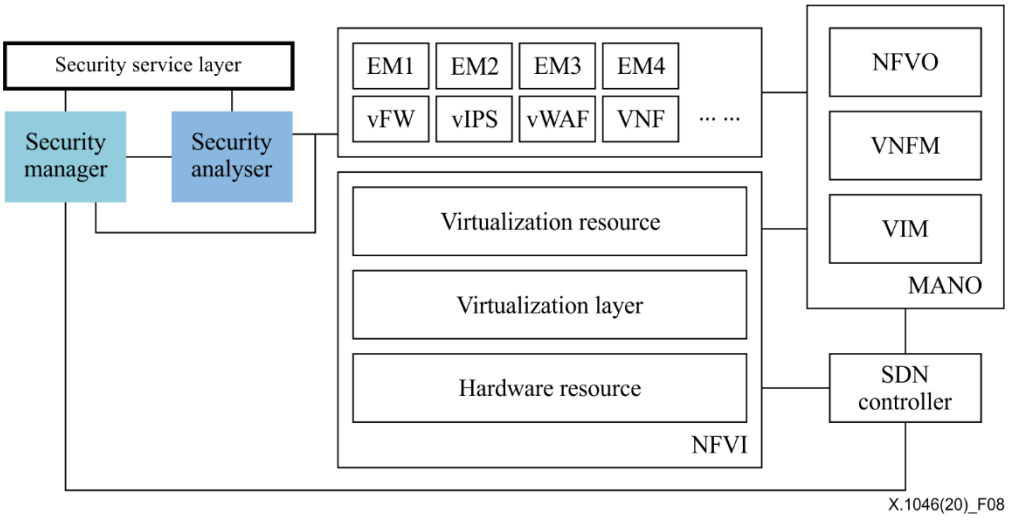

Figure 8 – Example of a software-defined security deployment in NFV environment

In an NFV environment, the security manager, the security analyser, the **security service layer**, virtualized security function instance, the *virtual network function manager (VNFM)* [b-ETSI NFV 003] and related interfaces can be deployed in the following ways:

1) Security manager: it can be a virtualized instance and deployed in virtual machines (VMs), or act as a physical device. With collaborating with NFVO [b-ETSI NFV 003], the security

manager can manage and orchestrate the security functions and security policies. The security manager can also integrate functions of element management system (EMS) [b-ETSI NFV 003] to manage and control the security functions and security policies directly.

2) VNFM: the VNFM in Figure 8 manages the lifecycle of VSF.

3) Security analyser: it communicates with the security manager, the security functions and the **security service layer**. It could be virtually implemented or be deployed as a physical device.

4) **Security service layer**: it provides security service to customers and can be integrated into the operation support systems (OSS) as a functional component of the OSS.

5) Virtualized security function instance: it is a security function which runs in VMs as a VNF or a VNF component) (VNFC) [b-ETSI NFV 003] of a VNF, e.g., a virtual firewall (vFW), virtual intrusion prevention system (vIPS), etc.

6) Interface between the security manager and the VNFM [b-ETSI NFV 003]: this interface is used when element management system (EMS) is integrated into the *security manager*. It uses the interface between EMS [b-ETSI NFV 003] and VNFM in [b-ETSI NFV 003] and [b-ETSI NFV 002].

7) Interface between the virtualized security function and the VNFM: it uses the interface between VNF and VNFM in [b-ETSI NFV 003] and [b-ETSI NFV 002].

10.2 Software-defined security deployment in SD-WAN

Software-defined wide area network (SD-WAN) technology applies SDN technology to WAN scenarios to realize automatic deployment of virtual private network (VPN) services and to accelerate the service deployment. To provide security service for the enterprise, the operator can deploy software-defined security components in SD-WAN. Figure 9 gives an example of security service provision by software-defined security in SD-WAN.

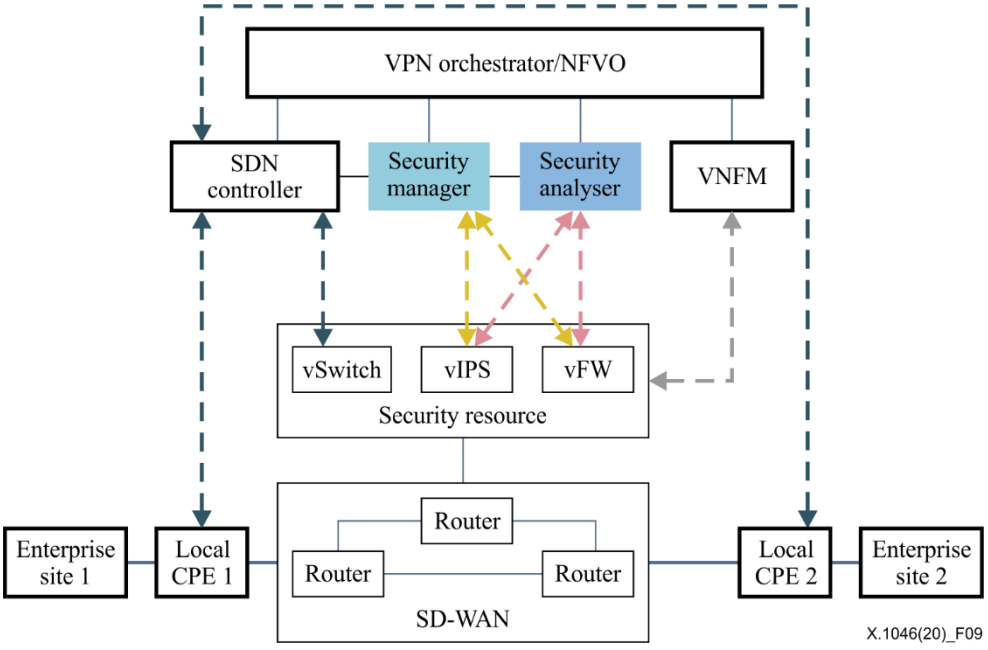

Figure 9 – Example of security service provision by software-defined security in SD-WAN

The forwarding policy and security policy of a VPN service for an enterprise can be sent to the SDN controller and the security manager respectively. The SDN controller sends the forwarding rules to the forwarding functions such as customer premise equipment (CPE) and virtual switch (vSwitch). The security manager resolves the security policy, selects applicable security function(s)

and configures related security policy in the selected security function(s). The security analyser analyses the security threats through analysing the security logs of the security functions and the network traffic. Then it provides security threat awareness to the enterprise. In this way, the software-defined security can provide security service to enterprises on demand.

Bibliography

[b-ITU-T X.1036] Recommendation ITU-T X.1036 (2007): *Framework for creation, storage, distribution and enforcement of policies for network security*.

[b-OASIS OpenC2-L] OASIS Open Command Open Command and Control (OpenC2) Language Specification Version 1.0. <https://docs.oasis-open.org/openc2/oc2ls/v1.0/cs01/oc2ls-v1.0-cs01.html>

[b-OASIS OpenC2-H] OASIS Specification for Transfer of OpenC2 Messages via HTTPS Version 1.0. <https://docs.oasis-open.org/openc2/open-impl-https/v1.0/cs01/open-impl-https-v1.0-cs01.html>

[b-OASIS OpenC2-P] OASIS Open Command and Control (OpenC2) Profile for Stateless Packet Filtering Version 1.0. <https://docs.oasis-open.org/openc2/open-impl-https/v1.0/cs01/open-impl-https-v1.0-cs01.html>

[b-IETF RFC 3176] IETF RFC 3176 (2001), *sFlow: A Method for Monitoring Traffic in Switched and Routed Networks*.

[b-IETF RFC 3917] IETF RFC 3917 (2004), *Requirements for IP Flow Information Export (IPFIX)*.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

[b-IETF RFC 8329] IETF RFC 8329 (2018), *Framework for Interface to Network Security Functions*.

[b-ETSI NFV IFA 010] Network Functions Virtualisation (NFV) Release 3; *Management and Orchestration; Functional requirements specification*. <https://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/010/03.04.01_60/gs_NFV-IFA010v030401p.pdf>

[b-ETSI NFV-SEC 003] ETSI GR NFV-SEC 003 (2016), *NFV Security; Security and Trust Guidance*. <https://www.etsi.org/deliver/etsi_gr/NFV SEC/001_099/003/01.02.01_60/gr_NFV-SEC003v010201p.pdf>

[b-ETSI NFV 002] Network Functions Virtualisation (NFV) (2014); *Architectural Framework.* <https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/012/03.01.01_60/gs_NFV-SEC012v030101p.pdf>

[b-ETSI NFV 003] Network Functions Virtualisation (NFV) (2018); *Terminology for Main Concepts in NFV* <https://www.etsi.org/deliver/etsi_gs/NFV/001_099/003/01.04.01_60/gs_NFV003v010401p.pdf>

[b-ONF SDN White paper] *Software-Defined Networking: The New Norm for Networks* (2012) <https://www.techylib.com/el/view/shapecart/software-defined_networking_the_new_norm_for_networks>

[b-RESTful] *RESTful Web Services - Introduction* <https://www.tutorialspoint.com/restful/restful_introduction.htm>

[b-UNISAFE] Taejune Park, Yeonkeun Kim, Seungwon Shin; UNISAFE: *A Union of Security Actions for Software Switches, ACM 2016, DOI*: <http://dx.doi.org/10.1145/2876019.2876025>

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, 2021