ETSI GS NFV-SEC 013 V3.1.1 (2017-02)

GROUP SPECIFICATION

Network Functions Virtualisation (NFV) Release 3;
Security;
Security Management and Monitoring specification

Disclaimer

The present document has been produced and approved by the Network Functions Virtualisation (NFV) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference

DGS/NFV-SEC013

Keywords

management, NFV, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights 5

Foreword 5

Modal verbs terminology 5

1 Scope 6

2 References 6
2.1 Normative references 6
2.2 Informative references 7

3 Definitions and abbreviations 7
3.1 Definitions 7
3.2 Abbreviations 8

4 Security Management Problem Statement 8

5 Security Monitoring Problem Description 8

6 Security Management 9
6.1 Introduction of Security Lifecycle Management 9
6.2 Gap Analysis for NFV Security 11
6.2.1 Current Model of Security Management 11
6.2.2 Policy Driven Security Management 12
6.3 High-Level Security Management Framework 13
6.4 Use Cases for Security Management 15
6.4.1 Overview 15
6.4.2 Single Operator Multi-Trust-Domain Use Case 16
6.4.3 Network Security Use Case 17
6.4.3.1 Introduction 17
6.4.3.2 Sub-Use Cases along Security Management Lifecycle 18
6.5 Security Management Requirements 20
6.5.1 Requirements for Multi-Trust-Domain Security Management 20
6.5.1.1 General Requirements 20
6.5.1.2 Functional Requirements for Security Management of Trust Domain 21
6.5.1.3 Requirements for Security Management 21
6.5.2 Requirements for Network Security Management 21
6.5.2.1 System Level Requirements 21
6.5.2.2 Functional Requirements 22

7 Security Monitoring 23
7.1 Security Monitoring Systems 23
7.1.1 Security Monitoring Classification 23
7.1.2 Security Monitoring Techniques 24
7.1.2.1 Overview 24
7.1.2.2 Passive Security Monitoring 26
7.1.2.3 Active Security Monitoring 27
7.1.2.4 Hybrid Security Monitoring 27
7.1.3 Limitations and Issues 27
7.2 Security Monitoring Use Cases 28
7.2.1 Deployment Scenario: EPC 28
7.2.2 Deployment Scenario: Network Based Malware Detection 29
7.2.3 Deployment Scenario: Subscriber Signalling 30
7.2.4 Deployment Scenario: IMS Network Monitoring 31
7.2.4.1 Overview 31
7.2.4.2 Security Issues 31
7.2.4.3 Security Monitoring the IMS Core Network 32
7.3 Evolving Trends Affecting Security Monitoring 32
7.4 Security Monitoring and Management in Virtualised Networks 33
7.4.1 Security Monitoring As An Infrastructure Capability 33

7.4.2 Data Access in Virtualised Environments 34
7.4.3 Non Standard Interfaces....34
7.4.4 Monitoring ETSI-NFV Defined Interfaces 35
7.5 NFV Security Monitoring & Management Requirements....36
7.5.1 Overview 36
7.5.2 Security Hardening Requirements 36
7.5.3 Securely Provisioning Security Monitoring Components....36
7.5.4 Secure Telemetry Access For Security Monitoring 37
7.5.5 Monitoring VNFs and Service Function Chains....37
7.5.6 Orchestrating Security Monitoring As A Service 37
7.5.7 Securely Auditing Security Monitoring....38
7.5.8 Operational Requirements 38
7.6 Security Monitoring and Management Architecture 38
7.6.1 Overview 38
7.6.2 Architecture Constructs 39
7.6.3 Security Monitoring System High-Level Flows 40
7.6.4 Secure VNF Bootstrapping Protocol....42
7.6.5 VNF Secure Personalization and Policy Protocol....47
7.7 NFV Deployments....51
7.7.1 Deployment Scenarios 51
7.7.2 vTAP Deployment Model....51
7.7.3 VNF Integrated Security Monitoring....52
Annex A (informative): Authors & contributors....53
History 54

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Group Specification (GS) has been produced by ETSI Industry Specification Group (ISG) Network Functions Virtualisation (NFV).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

In NFV network, network services and network functions can be deployed dynamically. The present document specifies functional and security requirements for automated, dynamic security policy management and security function lifecycle management, and Security Monitoring of NFV systems.

The main objectives of the present document are to:

- Identify use cases for NFV Security Lifecycle Management across Security Planning, Security Enforcement, and Security Monitoring.
- Establish NFV Security Lifecycle Management and Security Monitoring requirements and architecture.

Ultimate goal of this work: Scope of this activity is to study and investigate NFV security monitoring and management use cases and establish security requirements. The present document investigates passive and active monitoring of subscriber and management information flows, where subscriber information includes signalling and content.

Security Management and Monitoring are key components towards successful deployment of NFV. The requirements and results from the present document will act as catalyst towards rapid deployment of NFV.

Goals of the present document: The present document will recommend potential methodologies and placement of security visibility and control elements for fulfilling the requirements identified in the present document. The present document will be useful to VNF and VNFI providers, network operators and research community.

Non-goal: The present document does not address Lawful Intercept (LI). It may be applicable to performance and reliability monitoring for NFV systems.

Intended audience: VNF and NFVI providers, Network Operators, Service Providers, NFV Software Communities, SDOs (e.g. 3GPP, ETSI SC TC Cyber), Security experts and Researchers.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI GS NFV-SEC 001: "Network Functions Virtualisation (NFV); NFV Security; Problem Statement".

[2] ETSI GS NFV-SEC 003: "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance".

[3] ETSI GS NFV-SEC 012: "Network Functions Virtualisation (NFV) Release 3; Security; System architecture specification for execution of sensitive NFV components".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GS NFV-IFA 013: "Network Functions Virtualisation (NFV); Management and Orchestration; Os-Ma-Nfvo reference point - Interface and Information Model Specification".

[i.2] Richard Bejtlich, The Tao of Network Security Monitoring: Beyond Intrusion Detection, Addison-Wesley Professional, 2004.

[i.3] Chris Sanders and Jason Smith, Applied Network Security Monitoring, Syngress publications, 2014.

[i.4] PFQ.

NOTE: Available at https://github.com/pfq/PFQ.

[i.5] ETSI GS NFV 003: "Network Functions Virtualisation (NFV); Terminology for Main Concepts in NFV".

[i.6] ETSI GS NFV 002: "Network Functions Virtualisation (NFV); Architectural Framework".

[i.7] GSMA PRD N2020.01: "VoLTE Service Description and Implementation Guideline", V1.0, December 2014.

[i.8] Tomi Raty, Jouko Sankala, and Markus Shivonen: "Network traffic analysing and monitoring locations in the IMS," IEEE^{TM} 31st EUROMICRO Conference on Software Engineering and Advanced Applications (EUROMICRO-SEAA), Porto, Portugal, 30th August - 3rd September, 2005, pp. 362-369.

[i.9] Paolo De Lutiis and Dario Lombardo: "An innovative way to analyse large ISP data for IMS security and monitoring" IEEE^{TM} 13th International Conference on Intelligence in Next Generation Networks (INGN), Bordeaux, France, 26-29 October, 2009, pp. 1-6.

[i.10] Ari Takanen: "Recommendations for VoIP and IMS security" 3GPP Release 8 IMS Implementation Workshop, Sophia Antipolis, 24-25 November, 2010.

[i.11] D. Wang and Chen Liu: "Model based vulnerability analysis of IMS network," Academy Publisher, Journal of Networks, Vol. 4, No. 4, June 2009, pp. 254-262.

[i.12] ETSI GS NFV-REL 004: "Network Functions Virtualisation (NFV); Assurance; Report on Active Monitoring and Failure Detection".

[i.13] ETSI GR NFV-SEC 009: "Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI GS NFV 003 [i.5] and the following apply:

trust domain: collection of entities that share a set of security policies

Virtual Security Function (VSF): security enabling function within the NFV architecture

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GS NFV 003 [i.5] and the following apply:

AAA	Authentication, Authorization and Accounting
ISF	Infrastructure Security Function
ISM	Infrastructure Security Manager
NSM	NFV Security Manager
PSF	Physical Security Function
SEM	Security Element Manager
sNSD	security enhanced Network Service Descriptor
VSF	Virtual Security Function
WG	Working Group

4 Security Management Problem Statement

In NFV environment, network services and network functions can be created, updated, and terminated dynamically across multiple distributed NFVI-PoP. The site distribution and VNF/NS Life Cycle Management drives the demand for automatically aligning security policies with any changes of end-to-end network services in NFV environment.

However, security management techniques used for traditional, non-NFV deployments will not scale for NFV and may result in inconsistent security policies, inefficient processes and overall higher complexity, if applied in its current form to NFV deployments. With the deployment of NFV technologies, the networks are becoming increasingly flexible concerning the placement and the number of VNFs that are assigned to a specific network service. Security configuration on all different types of security functions has to be automatically adapted to the changing scenarios to ensure consistent security policies in sync with network service lifecycle management.

To achieve automated security management for NFV deployment, the concept of NFV security lifecycle management is introduced and studied in the present document for the establishment of consistent security policies and uniform enforcement of the policies across both virtualised and legacy networks.

5 Security Monitoring Problem Description

Operators and Service Providers continually need new tools and techniques to better manage their complex networks, and especially considering its dynamic evolution, including vastly diverse mix of endpoint devices and subscribers, dynamically changing content streams, and requirements for a vastly superior robustness and recovery. This natural evolution of the network necessitates a commensurate evolution in the ways future networks could be made more visible, and secure.

In traditional, non-virtualised deployments, a network operator correlates and analyses data collected from the user data plane and management and control planes. These correlated analytics assist the Operators to better manage their network, including ability to track the network usage, subscriber dynamics, content paths, SLAs, and any network threats and anomalies. Network borne attacks like exploitation of vulnerabilities, spreading of malware, exfiltration of data and service disruption can be detected and remediated. Certain collected probes can also provide network and user experience analytics, KPIs, and help address security impacts to the mobile customers, mobile carrier, and the downstream in general public. Any applicable threat remediation and countermeasures can then be deployed.

In non-virtualised deployments, many of the interfaces between the functional components are standardized and exposed, and hence the traditional active or passive probes can be used to monitor the packets, flows, configurations and any metadata in the management, data and control planes. These are used for performing security analytics, including deep packet inspection (DPI) functions and correlation. This type of monitoring mechanism is usually prevalent and applicable to different types of networks such as Operator's networks, IMS, enterprise networks and can be applied at different parts of the network, e.g. core and access. Traditional deployments generally have a single administrative control.

With the deployment of NFV technologies, the interfaces for security monitoring are not as distinct for access. These interfaces might be concealed by consolidated vertical "function silos" or by collapsed stacks like shared memory and virtual sockets, as opposed to using IP. ETSI NFV has published multiple virtualised models where these monitoring interfaces may be obscured. Access interfaces in the myriad deployments (e.g. within a VNF, or between multiple VNFs on the same hypervisor, etc.), make it difficult to probe the desired data for security monitoring. In some cases, deployments might implement vendor-proprietary, non-3GPP standardized interfaces to optimize processing power and reduce Signalling latency. In addition, security monitoring should comprehend and be effectively deployable within the ETSI NFV model that introduces multiple infrastructure and tenant domains.

NFV deployments have to provide an exceedingly greater level of Security Monitoring than in traditional non-NFV deployments, largely because NFV usages drive secure service delivery automation, live migrations, and orchestrated network and security management. In NFV deployments, orchestrators and controllers can automate virtual networks, virtual network functions and dynamic chaining, as well as applications. This diminishes the effectiveness of traditional physical security devices mostly because their lack of visibility into changes of the virtualised functions, service chains, and into the traffic being exchanged on virtualised platforms. A larger share of traffic is comprised of inter-VM traffic, also sometimes referred to as "East-West" traffic. In addition, virtual switches and virtual routers are increasingly being used for network policy and traffic re-direction. These policies, their associated configurations, management actions, faults and errors, and traffic shall be monitored for security assurances. The problem of security monitoring is the ability to view deeply into the entire network (virtual and physical), and deliver and enforce automated security monitoring management that is consistent with changes being applied by NFV orchestrators and VIM controllers.

This lack of visibility into management, control and data packets in an ETSI NFV virtualised system should be explored and addressed to enable the same robustness and visibility that exists in the current Operators networks. This includes security monitoring across the newly defined ETSI NFV interfaces, including all traffic for VNF management and control. In addition, the mechanisms should scale per the orchestration-based scaling of the NFV network, including a mixed deployment of NFV and traditional network functions.

In most cases, different trust domains have distinct and separate monitoring. For instance, Infrastructure Security Monitoring is administered by the Infrastructure provider to ensure that the NFVI is secure and robust for all Tenants. An administrator will have access to all NFVI security controls that can be impacted at the NFVI. A security goal of the Infrastructure providers is to ensure that the Tenant VNFs/VNFCs and Tenant traffic is not violating the NFVI established security policies, nor causing any malware proliferation into the NFVI or into other Tenants' assets. A Tenant's administrative domain is confine to the Tenant's VNFs/VNFCs and Tenant network. A Tenant can only monitor its own virtual network and ensure that the Tenant security controls are being met by the infrastructure. A Tenant does not have any knowledge of the NFVI nor of other Tenants. Existence of multiple trust domains and their distinct separation is a fundamental NFV deployment aspect and requirement. A uniquely subtle case is when the Operator has their own NFVI and run as a tenant as well. In these cases, Operators may still choose to keep the NFVI and Tenant trust domains as distinct (different departments running on same NFVI), or the same (Operator virtualizing their own Service Functions), depending on their Security Policies.

It is envisioned that the NFV environment will help providers build trust in their networks. One important aspect of that is protecting the subscriber experience. Maintaining proper security posture of the NFV infrastructure and subscribers' devices is an objective toward this end. As malware can waste significant amount of traffic, air time, and signalling resources, detecting and removing malware as early as possible is an important objective of security monitoring.

In addition to blocking attacks at the network perimeter, it is essential to minimize the insider attack surface (by detecting infected subscribers), assist in removing infected software, and quarantine infected subscribers. Conversely, detecting such weaknesses helps further reinforce perimeter protection. The NFV environment provides a unique opportunity for continuous monitoring that affects the combination of client- and network-security posture.

6 Security Management

6.1 Introduction of Security Lifecycle Management

NFV Security Lifecycle Management runs through three main stages: security planning, security enforcement, and security monitoring. Figure 1 is to clearly depict the three stages of security lifecycle and reflects the interlocking between them. These three stages are represented by three building blocks (Security Planning, Security Enforcement, and Security Monitoring) which constitute the security lifecycle.

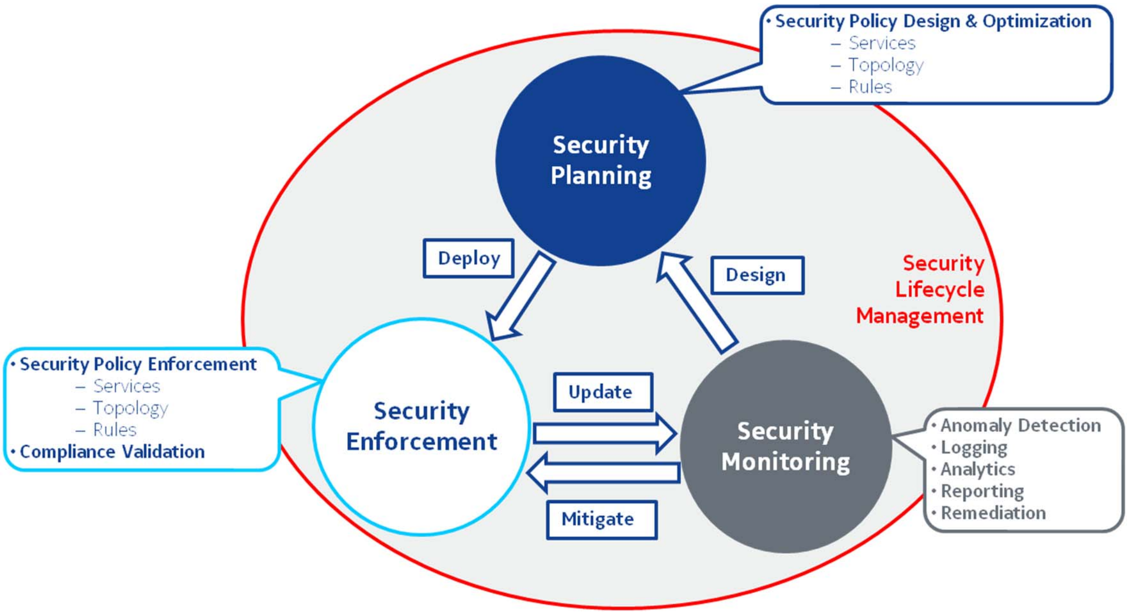

Figure 1

- Security Planning covers:
  - Manually or automatically design security policies for Infrastructure and/or network services based on security requirements, organization policies, etc.
  - Manually or automatically optimize security policies for Infrastructure and/or network services based on enhancement of organization policies, analytics results of monitoring, etc.
- Some examples of security policies are Network Access Control policy, Data security policy, Hardening policy, security monitoring policy, etc.
- Security Enforcement covers:
  - Manage Security Policies deployment and configuration changes in the:
    - ▪ Security Function.
    - ▪ NFVI.
    - ▪ VNF.
  - Automatically validate the compliance of the security policies.
- Security Monitoring covers the application and implementation of the security policy and achieving trusted assurances of that implementation through secure and trusted network security monitoring telemetry. Security Monitoring is elaborated in more details in clause 7.

In the present document, Security Planning and Security Enforcement are addressed and studied in the various use cases of security management (including policy management for security monitoring) in clause 6; while Security Monitoring is extended with more details in clause 7.

6.2 Gap Analysis for NFV Security

6.2.1 Current Model of Security Management

OSS, as a traditional management entity, is currently lacking security management capabilities for NFV deployment. So far in ETSI NFV, the management services supported by the reference point between OSS and NFV Orchestrator (Os-Ma-nfvo) only cover performance management and fault management for network services, but not security management [i.1]. Network service deployment is automated by NFV-MANO without explicitly considering security management for network services. I.e. neither OSS nor NFV-MANO is able to provide security management for network services and infrastructure in NFV environment currently.

Seen from a technical point of view, two different approaches for virtual security functions can be distinguished: the VNF-based approach and the NFVI-based approach. In the present document, the term VSF (Virtualised Security Function) denotes a virtual security function via a VNF-based approach; the term ISF (NFV Infrastructure - based Security Function) denotes a security function or security feature provided by the NFVI.

Besides virtual security functions, traditional security functions like physical firewalls are also needed, because otherwise the network layers beneath the virtual security functions would remain unprotected. In the present document, the term PSF (Physical Security Function) denotes a physical security function.

With the current possibilities for security management, the following actors (comprising machines as well as human beings) would be involved:

- Administrator - security administrator (human).
- NFVO.
- VNFM.
- VIM.
- EM.
- VSF (VNF-layer Security Function).
- ISF (NFVI-layer Security Function).
- PSF (Physical Security Function).

The virtual security functions (VSF and ISF) and physical security functions (PSF) are managed and configured as follows:

- VSF (e.g. vFW in VNF layer) is managed by the administrator through the VNFM/EM:
  - instantiated and lifecycle managed via the VNFM, configured via associated EM.
- ISF (e.g. vFW in NFVI layer) is managed by the administrator through the VIM.
- PSF (e.g. traditional pFW) is managed by the administrator through associated EM.

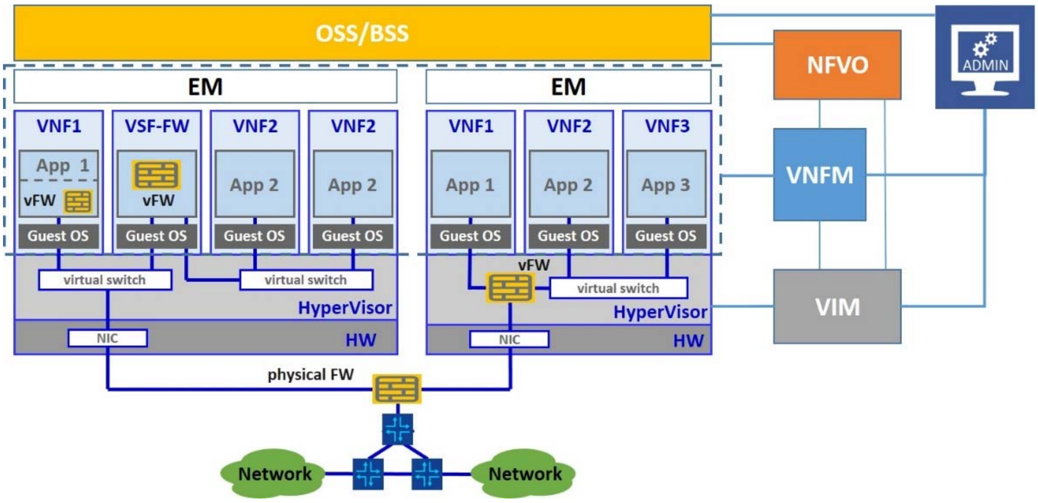

Figure 2: Current Model of Security Management

In NFV deployment, the VSFs (e.g. vFWs, virtual SEC-GWs, etc.) controlling the traffic to the VNFs need to be instantiated, (re-)configured, or terminated or migrated dynamically along with the VNFs that shall be continuously protected. Without proper automation of security management, the following actions have to be triggered/performed manually by the authorized administrators (assuming proper security policy for network access control is already designed offline and made available to administrators):

- The required VSFs have to be instantiated manually by an authorized administrator via the VNFM after the network service is deployed by the NFVO, if they are not included in the network service descriptor. Also the configuration on the instantiated VSFs has to be performed by the administrator via the EM.

- Whenever VNFs assigned to the network services are migrated, the VSFs (controlling the traffic to the VNFs) may also need to be migrated or re-configured. While VNF migration can be automated by the MANO blocks, the migration & configuration of VSFs have to be conducted by the administrator if VSFs are not already part of NSD, as specific security considerations shall be taken into account.

- When the network service is scaled, new VNFs may need to be instantiated and existing VNFs may need to be terminated. While VNF handling can be automated by the MANO blocks, the instantiation/termination of the VSFs (controlling the access to the VNFs) will have to be triggered by the administrator via the VNFM.

- The configuration of the NFVI-based security functions (e.g. hypervisor-based FWs) has to be performed by the administrator via the VIM.

- The configuration on the traditional physical security functions (e.g. conventional FWs) between infrastructures has to be performed by the administrator via the EM.

The above manual actions are inadequate and are error-prone as they require continuous, concentrated and consistent manual interaction of administrators. Moreover, they are not scalable, cumbersome to execute and may require frequent re-calibrations. Manual steps slow the deployment processes for securing network services or lead to security weaknesses, and occasionally personnel do not have the knowledge to quickly adapt security measures to new situations. These are the typical gaps resulting from 'current, manual security management' when faced with NFV related dynamicity, complexity, and mobility challenges.

6.2.2 Policy Driven Security Management

The security management processes in clause 6.2.1 can significantly be improved by policy driven security management tasks, extending and cooperating with the existing MANO tasks specified so far. In particular, very similar to the automation of network service management realized by MANO blocks, there is urgent need for automation of security management too, in order to assure high quality and speed of security management. Such highly specialized security management tasks require a security specific logical functional block, where the functionality can be executed in a protected, automated and consistent manner.

Automated security management addresses the problems in clause 6.2.1 as follows: involved administrators only need to interact with a logical functional block for security management during a security policy design phase. Once security policy design is completed, the security management functional block enforces the designed security policies in automated manner barring exceptional conditions.

When authorization from tenants is needed for the security policy enforcement, the security management functional block should allow the tenants to decide whether the security policy will be enforced.

In security policy design phase, security functions across domains (including VSF, ISF, PSF) may need to be included for protecting a specific network service. The configuration information of each security function may also be specified in the security policy.

Security policy enforcement has two aspects:

1) Lifecycle management (instantiation/scaling/migration/termination) of VSFs required for the network service.

2) Configuration of all security functions required for the network service (including VSF, ISF, PSF).

During network service deployment, VSFs are instantiated before the VNFs belonging to the network service. Before VNFs for a network service are deployed, the Network Services Descriptor (NSD) security parameters are populated based on the security policies. Hence the network service can be deployed with appropriate security functions by the NFVO. Automated Security enforcement, per trust domain, for Network Services may entail:

- lifecycle management of VSFs and configuration on VSFs;
- configuration on NFVI-based security functions;
- configuration on traditional physical security functions;
- adaptation of security policy enforcement due to network service scaling/updating, etc.;
- adaptation of network service security in case of unforeseen events (e.g. when triggered from security monitoring and analysis tasks).

In case that the security functions or parameters from the security design phase are not suitable or not enough, alternative approaches should be supported to update the security functions or parameters, e.g. through EM. As automated security policy management co-exists with MANO blocks, security controls implementing the security principles [i.12] of:

a) separation of privileges;

b) least privilege; and

c) least common mechanism may be used to separate the scope of management responsibilities between security administrators, the aforementioned logical function block for security management and MANO blocks and to protect against unauthorized privilege escalation and privilege misuse threats that may stem from the interdependences between security policy management and MANO.

6.3 High-Level Security Management Framework

As explained in clause 6.2, security protection of NFV network services necessitates security functions like Virtualised Security Functions (VSFs) and NFVI-based Security Functions (ISFs), as well as Physical Security Functions (PSFs). For managing and monitoring those security functions with a certain level of automation, NFV Security Management (NSM) functionality is required to cope with inherent complexity, separation of domains and consistency challenges of security management for network services across these domains. The shaded areas in figure 3 show the high-level Security Management Framework as a logical extension to the current NFV framework.