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

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

Contents

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™ 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™ 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.

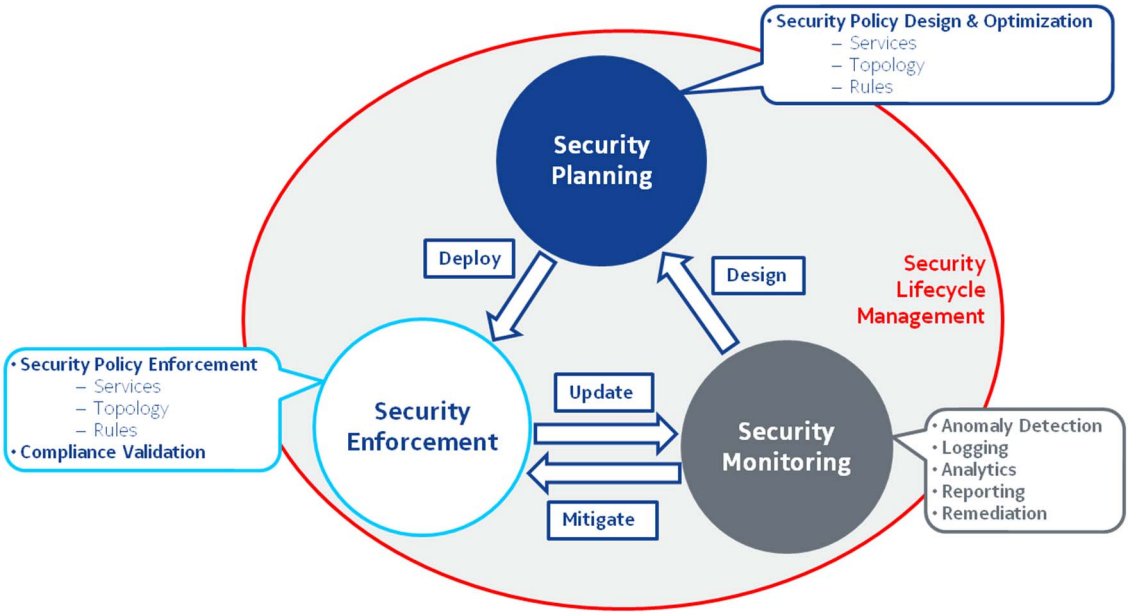

Figure 1

- 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.

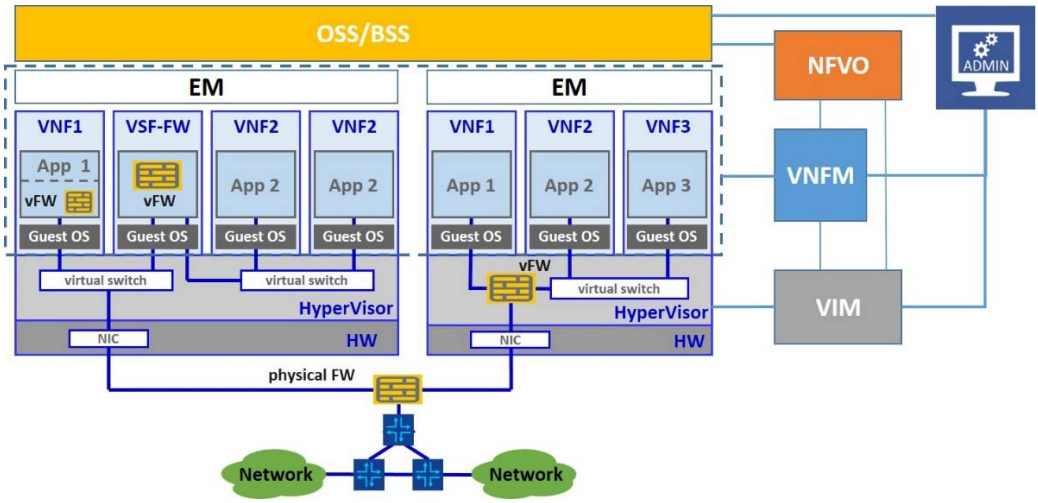

Figure 2: Current Model of Security Management

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.

The major difference of NSM from NFV-MANO is the clear focus on security tasks including security functions realized in the physical network part, i.e. NSM manages not only the security functions in virtualised network, but also security functions in traditional physical network to enhance the overall protection level. The main building blocks for NSM in addition to those in the current NFV framework comprise:

- **Virtual Security Function (VSF)** running on top of NFVI, which is a special type of VNF with tailored security functionality (e.g. firewall, IDS/IPS, virtualised security monitoring functions like vFEP, vTap). VSFs are mainly required to protect the other VNFs, which constitute a network service. VSF is managed by either dedicated VNFM or generic VNFM with respect to its lifecycle.

- **NFVI-based Security Function (ISF),** which is a security function provided by the NFV Infrastructure. It includes virtualised security appliances or software security features (e.g. hypervisor-based firewalls) and hardware-based security appliances/modules/features (e.g. Hardware Security Modules, Crypto Accelerators, or Trusted Platform Modules).

- **Physical Security Function (PSF),** which is a conventionally realized security function in the physical part of the hybrid network. Even if a telco network is virtualised, additional PSFs are still needed, for instance to protect the NFV infrastructure (and inherently, the Network Services running on top) as a whole. PSF is part of the non-virtualised traditional network and not maintained by the NFVI provider, hence it is managed by the SEM instead of the VIM.

NOTE 1: The PSF is included in the present document in order to show the complete security architecture of a full network. However, the location, functionality and interaction with a PSF is outside the scope of the present document.

NOTE 2: SEM refers to Element Manager managing Security Functions.

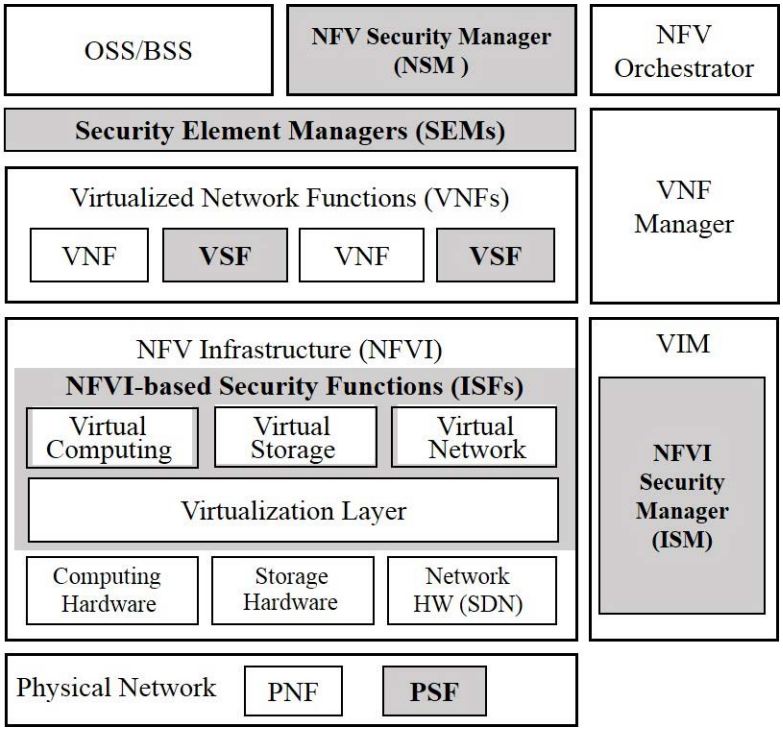

Figure 3: High-Level NFV Security Management Framework (in grey)

- **NSM** is the logical functional block for overall security management, e.g. on the behalf of network services. In cooperation with MANO blocks dedicated to managing the virtualised network, the policy driven NSM is specialized to manage the security on a network service over its entire lifecycle. It covers the following functionalities:

  - **Security Policy Planning**, where the term **Security Policy** involves the following elements:

    - Security Functions (including VSFs, ISFs, and PSFs).

    - Configuration information (e.g. credential types, security rules on each security functions).

- Topology information of secured network services.

Security Policy Planning function designs and optimizes security policies for specific targets of protection (e.g. network services) through possible co-ordination between multiple NSMs. Usually, the planning phase is not fully automated, but requires assistance from security administrator, who designs security policy following recommendations from an initial security assessment and/or security related policies coming from other sources (e.g. operator's general policy of deployment, threat and risks analysis for the network service, etc.) The designed security policy is also used for compliance validation after security policy enforcement.

- **Security Policy Enforcement & Validation:** Security Policy Enforcement function automates the deployment and supports lifecycle management of security functions as defined in the design phase, then configure security policies on the security functions. In addition, during lifetime of a network service, the validation and re-configuration/remediation of associated security policies is supported, also in automated manner.

- **ISM** is the logical function dedicated to security management in NFVI layer. It builds and manages the security in NFVI to support NSM requests for managing security of network services in higher layer.

There shall be security controls in place (e.g. security and privileged access management controls) that ensure separation of concerns, duties and privileges between MANO and NSM as well as the administration of individual security functions and NSM. For example, NSM may be responsible for coordinating the life-cycle of security functions and maintaining the association between security function and policy, and validating conformance between security policy enforcement and network topology. The security function administrators may be responsible for defining security rules and policies as well as constraints about the validity of the enforcement of the security policy (e.g. dependencies between VSFs such as relative order or chaining of security VSF). The components in the MANO subsystem may be responsible for on-boarding new VSF packages, the life-cycle management of the VSF packages (including the execution environment configuration of VSF packages but not the security policy rules of the VSFs), the management of resources associated with these and NFVI resource requests. The security principles [i.12] of:

a) separation of privileges;

b) least privilege; and

c) least common mechanism shall apply to reduce the attach vector of the management layers and mitigate the risk of unauthorized privilege escalation.

6.4 Use Cases for Security Management

6.4.1 Overview

The use cases in clauses 6.4.2 and 6.4.3 can be understood as typical security management tasks that need to be supported by an NFV security management system. There may be other security management tasks as well, however, in the present document a limited number of use cases are considered for illustration. They should be expressive enough to demonstrate principle usage of involved entities and interfaces for specific security management functions, and sufficient enough to identify the requirements for NFV security management in clause 6.5.

6.4.2 Single Operator Multi-Trust-Domain Use Case

In typical NFV environment, a telco network deployed by an operator normally can involve multiple tenants and stretch across multiple infrastructures, especially in hybrid scenario or multiple-cloud scenario which may contain private and public clouds. A single trust domain NFV deployment across is more vulnerable to any security breaches as an attack on any single element anywhere in the service chain may compromise the entire deployment. This is particularly essential for Critical Network Infrastructure (CNI) and networks built with sensitive network functions for supporting e.g. LI and RD applications. Therefore, proper protection is needed by segmenting the deployed network into different trust domains, to keep data traffic away from management traffic and separate network functions from each other according to different security requirements. The split of multiple domains may for instance include different types of VNFs or different layers such as the service layer or the infrastructure layer.

In order to ensure security management and monitoring system to be multi-trust capable while avoiding too much complexity with full array of possible multi-trust-domain scenarios, the present document mainly addresses a concrete simple multi-trust-domain use case that cover the horizontal trust split, as follows:

- Single network operator with multiple trust domains:
  - Taking the example of IMS service to highlight the level of NFV complexity, for important scenarios for CNI (Critical National Infrastructure) and LI (Lawful Interception), where the IMS network in NFV environment is segmented in multiple trust domains.

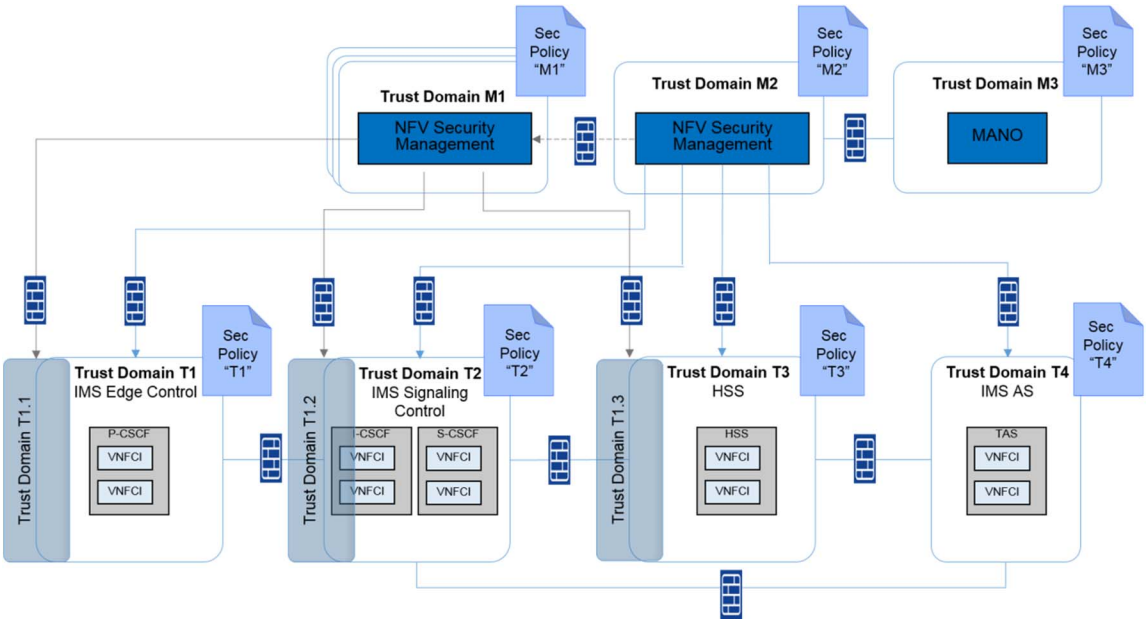

Figure 4: IMS Service deployed by a Single Network Operator with Multiple Trust Domains

As shown in figure 4, a telco operator separates and groups different types of network functions for IMS service (VNFs in NFV deployment) into different trust domains according to their different security levels and requirements. In this example, VNFs for IMS Edge Control are grouped in Trust Domain T1; VNFs for IMS Signalling Control are grouped in Trust Domain T2; HSS VNF alone is isolated in Trust Domain T3; VNFs for AS/TAS are grouped in Trust Domain T4. To separate data plane from management plane, management entities are also grouped into different trust domains. Considering their different functionalities and security sensitivity, Security Management and MANO entities are further isolated into separate Trust Domains of M2 and M3 respectively. The arrow in figure 4 denotes the direction of control.

Further to support the isolation of special sensitive functions supporting e.g. LI application, there is also a dedicated trust domain M1 containing an entity that manages security of the specific functions, which are further grouped into dedicated overlay trust domains like T1.1, T1.2, T1.3.

For interaction between different trust domains, trust relationship between trust domains are defined in the forms of security policies including e.g. access control policies, policies for traffic/resource separation and segmentation, setting up VPN SeGW, etc.

6.4.3 Network Security Use Case

6.4.3.1 Introduction

In NFV environment, virtualisation features pose unique and specific security challenges for tenant/service isolation, traffic/data and code protection, e.g. due to sharing of resources among potentially multiple tenants or services. Hence, network security is of major importance and shall be provided for NFV deployment of network services. All the measures for network security in traditional networks like structuring of a network into different security zones, separation of the traffic into different traffic classes, and utilization of security instances like firewalls or IDS/IPS, have to be applied in NFV environment as well.

Heterogeneity of services in NFV environment demands to adopt varying degrees of granularity in network security mechanisms. The network security use case in the present document is dealing with e.g.:

- Interface separation, traffic separation and segmentation.
- Traffic filtering (FW).
- Security zone assignment/DMZ.
- Building secure channels for VPN, IPsec or https, etc. (e.g. VPN-GW, SEC-GW).

Traffic routed through a virtualised network may not be completely visible to traditional security inspections as previously applied on physical networks. This raises the need for virtual security appliances like virtual firewalls or virtual IDS/IPS to achieve a level of security comparable to that in traditional networks. Besides the virtual security appliances, traditional security appliances like physical firewalls are also needed, because otherwise the network layers beneath the virtual security appliances may remain unprotected.

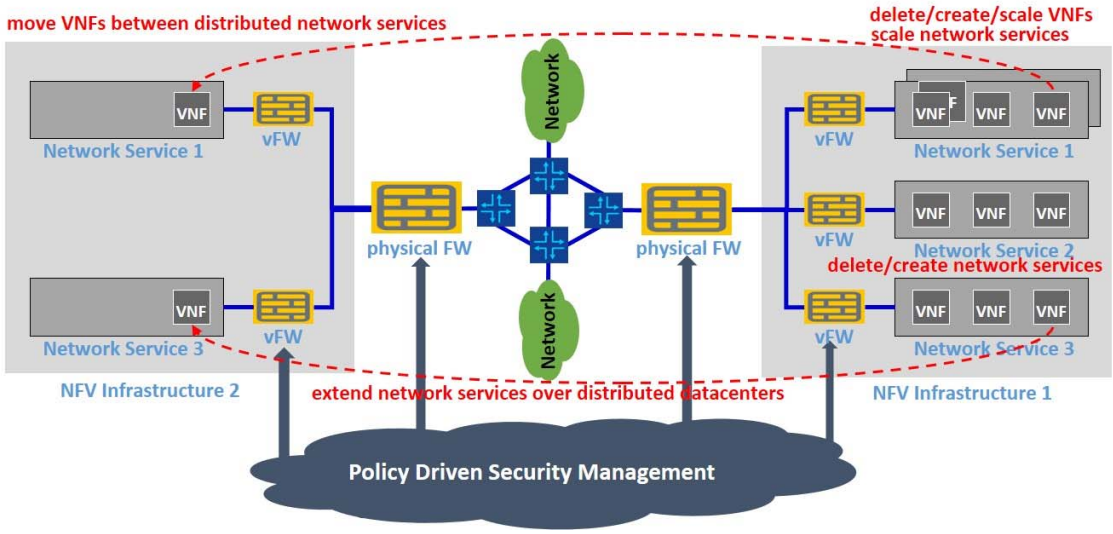

Figure 5: NFV deployment with dynamic network security configuration and policy alignment

Assuming a situation as shown in figure 5 (here with the example of virtual firewall (vFW)), the external physical FWs pass the traffic for all network services running on the NFV infrastructures and may block all other traffic; vFWs inside the NFV infrastructures independently restrict traffic to the dedicated virtualised network services (policy governance may be common across the firewalls). If now a new network service is created, or an existing one is removed, or a running network service is scaled-out/scaled-in or even extended over distributed datacentres, or VNFs are moved between distributed network services, it will be necessary to ramp down/update the existing vFWs or to create new vFWs, depending on the security requirements of the resulting mapping of NFV to datacentres. To constantly assure adequate security for network services, this implies that security policy needs to be adapted. This can be achieved by means of "Policy Driven Security Management", which may coordinate network security policies in- and outside of the NFV environment.

6.4.3.2 Sub-Use Cases along Security Management Lifecycle

Network security management is closely associated with security lifecycle management as introduced in clause 6.1. Network security use case consists of the relevant sub use cases related to design and enforcement of network security policies, which influence creation, updating, configuration and termination of security functions protecting an individual network service.

Following security management lifecycle phases, the present document distinguishes between security policy design and security policy enforcement, where the latter is sub-divided into a set of enforcement use cases, which depend on lifecycle stage (ready for deployment, already deployed, running, updated) of an individual network service. As shown in the figure 6, security policy sub use cases are initiated on certain triggers from network management and security management, e.g. driven by administrators of the NFVO and the NSM.

In security policy planning stage, a security policy is designed for a specific network service type (sub-UC-d: Policy Design). This sub use case is initiated by administrators supported by security experts, since to a certain extent the design process requires human interaction and security knowledge. Once designed, a security policy is prepared to protect an individual network service to which it is assigned.

While it may be necessary to adapt or change policy enforcement after service deployment, an initial security policy enforcement shall be applied before services are deployed. Refer to sub use case e1, e2, and e3.

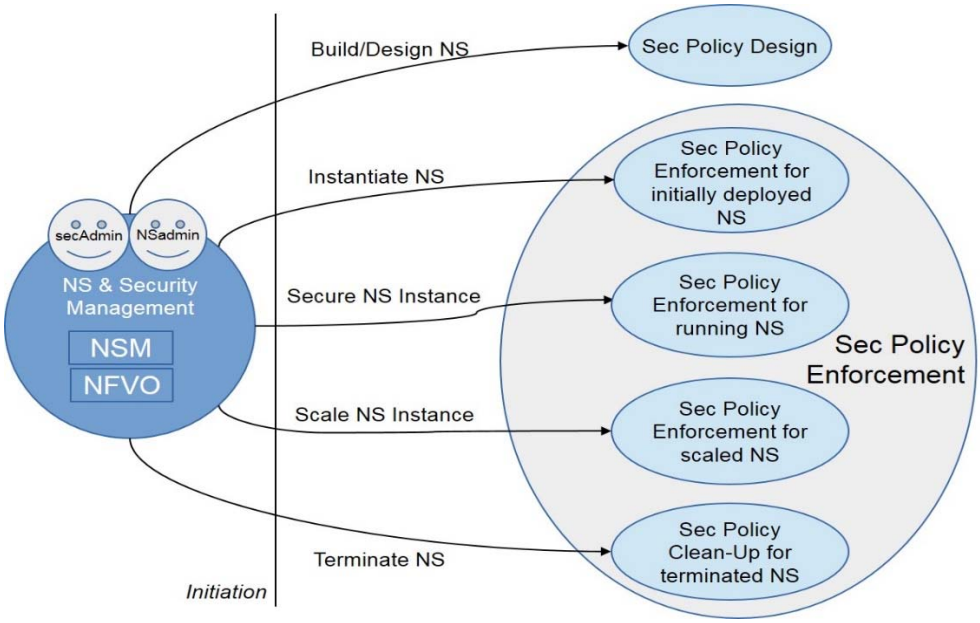

Figure 6: Network Security Use Case Breakdown into Sub Use Cases

1) sub-UC-d: 'Policy designing for network services'

In the preparation phase, the network security policy is designed based on relevant industry standards, network service specific threat and risk analysis, organizational polices, availability and characteristics of security functions, etc. Consequently, the Network Service Descriptor (NSD) describing the topology of the virtualised network will be enhanced with the security information in the policy. Figure 7 illustrates the flow of information for the generation of security policies and the enhanced NSD containing the security information (called sNSD thereafter in the present document).

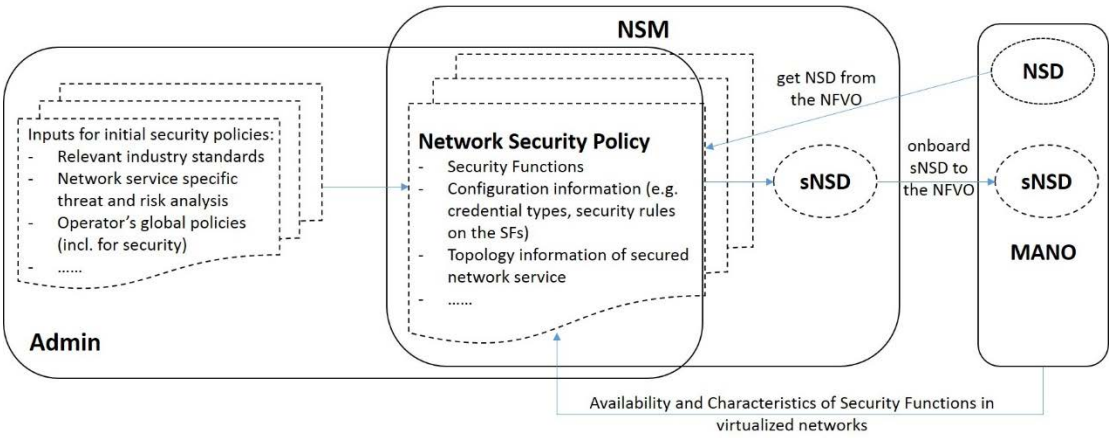

Figure 7: Generation of Security Policy and sNSD

2) NS policy enforcement for network services is performed depending on actual network service deployment, including:

sub-UC-e1: 'Policy enforcement for initially deployed network service'

This sub use case describes the procedure of automated network security policy enforcement for an individual network service (of a defined type) with an associated policy based protection already prepared in the design phase. As the individual network service is not instantiated yet, the prepared sNSD (associated to the specific network service type) is now enforced during deployment of the network service. In this process, security functions are created and configured at the beginning of network service lifecycle (i.e. network service instantiation). Figure 8 illustrates the information flows involved during the enforcement procedure.

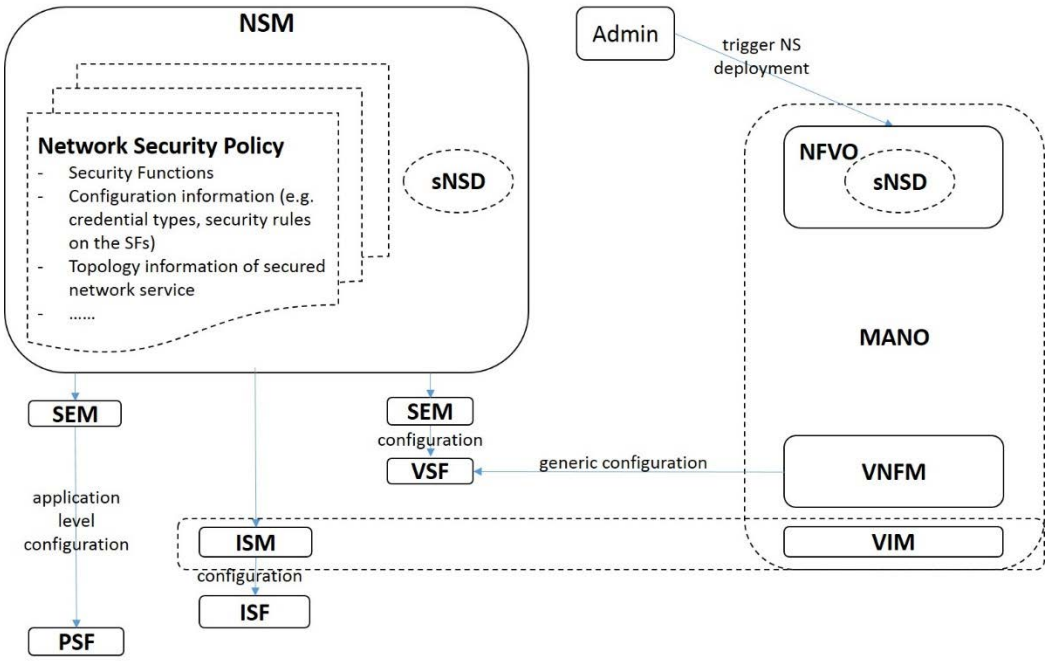

Figure 8: Policy Enforcement for initially deployed network service

sub-UC-e2: 'Policy enforcement for scaled network service'

This sub use case describes the procedure of automated network policy enforcement during scale-in or scale-out of a network service. The security functions will be terminated or created and/or configured in the middle of network service lifecycle following to the network security policy already available in the NSM. Figure 9 illustrates the information flows involved while the security policy is enforced due to network service scaling.

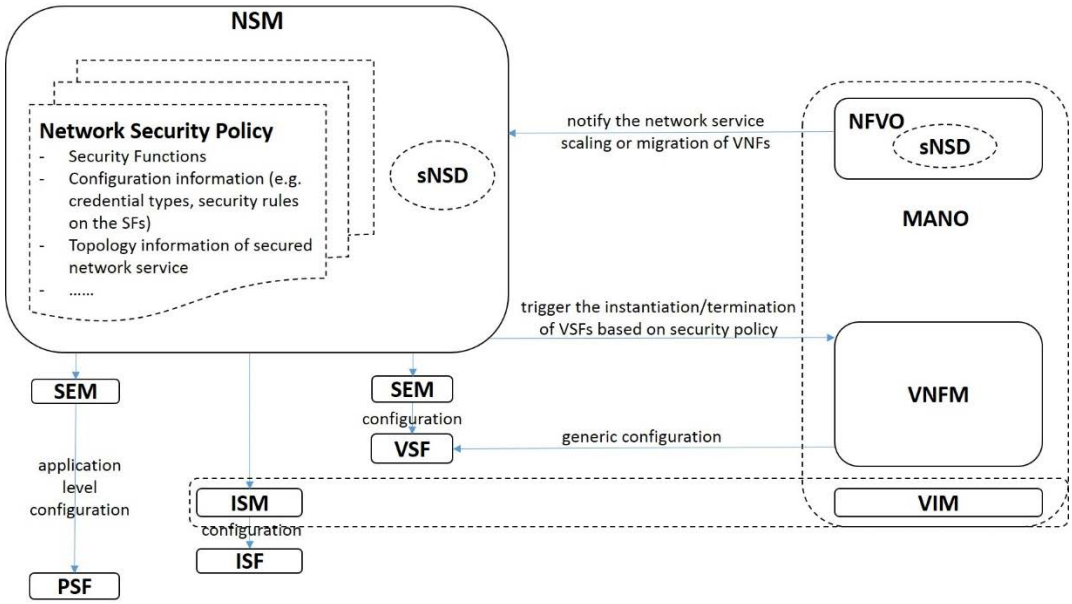

Figure 9: Policy Update due to network service scaling

sub-UC-e3: 'Policy clean-up for terminated network services'

This sub use case describes the procedure of automated network policy clean-up after the network service is terminated. Any relevant configuration held in either virtual or physical components should be removed.

In the case where the VSF/ISF is dedicated to a single service (which is being terminated), then the VSF shall be terminated as part of NS removal by the NFVO. In the case of an ISF, the ISF can be terminated when it is instantiated as a VNF or otherwise cleaned up if the ISF is not instantiated as a VNF.

In the case where the VSF/ISF is shared across multiple services, the policies shall be updated as described in clause 6.4.3.2 to enforce the correct policies for the remaining service(s).

Any credentials stored in NSM for VSF's are also removed on notification from NFVO. If Security Policy requires retention of any data (including logs), it is preserved by the NSM.

6.5 Security Management Requirements

6.5.1 Requirements for Multi-Trust-Domain Security Management

6.5.1.1 General Requirements

The requirements listed in this clause are general requirements for setting up and securing multiple trust domains described in clause 6.4.2:

R1. Entities (e.g. VNFs) building up telco networks (e.g. IMS network)shall be assignable to different trust domains.

R2. One or more dedicated MANO trust domains shall exist.

R3. Each MANO entity shall be assignable to one or more of the MANO trust domain.

R4. Trust Relationships shall be defined between trust domains.

R5. For two or more domains without existing trust relationships, the effect of an attack on one domain shall not impact the other domains either directly or indirectly (e.g. through Management channels).

R6. There shall be one or more NFV Security Managers, per trust domain.

R7. There shall be controls enforcing separation of duties and privileges, least privilege use and least common mechanism between security management and MANO. These controls shall apply in conjunction with the corresponding separation of trust domains.

6.5.1.2 Functional Requirements for Security Management of Trust Domain

The requirements listed in this clause are functional requirements for trust relationship management between trust domains, as well as trust management within a single trust domain:

R8. A NFV Security Manager shall manage security policies and implement the security requirements of a Trust Domain to be implemented by the dedicated security functions or security functions embedded within VNFs:

- Security requirements and policies of a trust domain or VNFs in the trust domain shall be built in the descriptors and could include e.g. traffic separation and segmentation, firewalls, secured platform, encryption service, hardware security requirement, VNFC placement, hardening, security monitoring, etc.

R9. A NSM shall manage security policies and requirements between trust domains according to the defined trust relationship, including establishing security association between VNFs in different trust domains and between VNFs and MANO entities when it has visbility and permissions available to perform such duties:

- Security policies reflecting trust relationships between trust domains could include access control (Authentication & Authorization), traffic/resource separation and segmentation, VPN SeGW, etc.

R10. A NSM shall manage security policies within a trust domain, including establishing security association between VNFs within a single trust domain:

- Security policies within each trust domain included e.g. initial key provisioning for secure communication between VNFs, Authentication & Authorization, firewalls, etc.

R11. NSMs shall be able to interact (where authorized) with each other for requesting/providing required security services for e.g. cross-domain security management.

6.5.1.3 Requirements for Security Management

The requirements listed in this clause are security requirements for protecting security management functional blocks:

R12. One or more dedicated trust domains for Security Management shall exist.

R13. NSM shall be assignable to one of the dedicated Security Management trust domains.

R14. The NSM shall be instantiated on a host system which meets the requirements laid out in ETSI GS NFV-SEC 012 [3].

R15. The NSM may be deployed as virtualised workload.

R16. Traffic of NSM shall be isolated and separated from other traffics in data/control planes, etc.

6.5.2 Requirements for Network Security Management

6.5.2.1 System Level Requirements

The requirements listed in this clause are system level requirements for NFV security management:

R1. The NFV security management system shall support the security lifecycle management as introduced in clause 6.1:

- The security management system shall support capabilities allowing operators to perform security policy planning for network services, which includes security policy initial design and optimization.

- The security management system shall support a capability allowing operators to enforce (including validate) the designed security policies throughout the network service lifecycle.

- The security management system shall support a capability allowing operators to perform security monitoring as described in clause 7.

R2. The Operator's security management system shall support a capability to manage security functions in both virtualised and physical networks within bounds of trust domains.

R3. The NFV security management system shall support a capability allowing operators to automate the above functions.

6.5.2.2 Functional Requirements

The requirements listed in this clause are functional requirements for realizing the use cases described in clause 6.4.3. These requirements are mainly imposed on the logical functional block for security management (i.e. NSM), NFV-MANO blocks, and other management entities:

- **To perform security policy design procedure, the following requirements need to be met:**

  R4. To facilitate security policy design, the NSM shall support checking the availability and capabilities of VSFs and ISFs (via ISM), as well as PSFs (via the associated EM(s)).

  R5. The NSM shall support extending Network Service Descriptor (NSD) with the security information contained in the designed security policies to create sNSD.

  R6. The sNSD shall support the security zone/placement, the connectivity and the description of the VSFs needed for controlling the traffic to VNFs.

  R7. The sNSD shall be made available to the NFVO for deploying network services with security protection.

- **To perform security policy enforcement procedure, the following requirements need to be met:**

  R8. If sNSD is available before a network service is deployed, the sNSD shall be used by the NFVO for initial deployment of the network service. The VSFs (e.g. the virtual firewalls included in sNSD) for protecting the network service are instantiated together with the VNFs assigned to the network service.

  R9. If sNSD is not available before a network service is deployed, the NSM shall be able to get the information of the deployed network service (or VNFs) from the NFVO for applying security policies to the unprotected network service.

  R10. To enforce security policies on unprotected network services, the NSM shall be able to trigger the instantiation of the required VSF(s) (via the VNFM) according to the designed security policies and update network topology accordingly.

  R11. For updating the enforced security policies when network services are scaled-in/scaled-out, the NSM shall be informed (by the NFVO) of the result of the scaled network services.

  R12. The NSM shall be able to trigger the instantiation of new VSF(s) required for protecting the instantiated VNF(s) for scaled network service or termination of affected VSF(s) via the VNFM, based on the designed security policies.

  R13. The NSM shall have the capability to configure security rules on VSFs/PSFs (via the associated EMs) and ISFs (via ISM) following the designed security policies.

  R14. Network Security Management shall provide an interface from the NSM to the VSFs/PSFs (via the associated EMs) and ISFs (via ISM) to allow configuration of the instantiated VSFs (e.g. initial credentials, etc.).

  R15. The NSM shall have the capability to configure security policy validation for the deployed/scaled network services.

  R16. Network Security Management shall provide an interface from the NSM for security policy validation for the deployed/scaled network services.

  R17. The NSM shall have the capability to clean-up of enforced security policies related resources for the terminated network services.

R18. Network Security Management shall provide an interface from the NSM for the clean-up of enforced security policies related resources for the terminated network services.

7 Security Monitoring

7.1 Security Monitoring Systems

7.1.1 Security Monitoring Classification

Security monitoring may be broadly classified into Management Security Monitoring, Service Security Monitoring and System Security Monitoring. Management Security Monitoring includes such as access attack monitoring, operation behaviour monitoring, deployed security policy monitoring. Service Security Monitoring includes service interface security monitoring and service treatment security monitoring. System Security Monitoring includes system integrity, resource usage and trafficmonitoring.

1. Management Security Monitoring

Management security monitoring focuses on the security monitoring actions to the Management plane in NFV scenario, including but not limited to the following:

- Access attack monitoring:
  - Various behaviours of connection and login attempts are monitored and audited to detect access attacks and potential access attempts and to take actions accordingly.
- Behaviour monitoring:
  - Behaviour in various operations by authorized account access after login is monitored and audited to detect mistakes, malicious operational activity.
- Security Policy Integrity Monitoring:
  - The configuration of security parameters is monitored and audited to see if it complies with the security policies as defined, and to see if vulnerabilities are discovered after deployment, or if they are tampered with.

2. Service Security Monitoring

Service security monitoring focuses on the service plane for NFV scenarios:

- Service interface security monitoring:
  - The attacks to service interfaces exposed externally to the system are monitored and audited, e.g. illegal access, in order to detect the attacks to the service interfaces so that correct measures can be taken, such as implementing security hardening.
- Service treatment security monitoring:
  - Various attacks detected in the service handling procedure are monitored and audited, e.g. malformed messages, signalling flooding and replaying, etc., in order to detect the attacks to the services and take actions accordingly.

3. System Security Monitoring

System security monitoring provides monitoring functions to the whole system, so that some security events from all layers can be detected:

- System Integrity Monitoring:
  - It refers to the monitoring and auditing of any unexpected or unauthorized processes run in the system. In NFV environment, due to the openness of the system, and the dynamic lifecycle management, the possibility of embedding unauthorized software/process is increased, which makes the monitoring and audit more important.
- Systems Logs Monitoring:
  - Logs from various applications, VNFs, infrastructure elements and workloads are monitored (where authorized) to detected anomalies in the system components.
- System Traffic Monitoring:
  - Traffic patterns and volumes need to be monitored to detect inbound or outbound DoS attacks, and also to prevent malware download attempts.
- System resources usage monitoring:
  - Resources allocated dynamically during lifecycle management in NFV environment are monitored to reduce the risks of resources misuse, e.g. increasing additional resources during allocation, un-releasing or releasing less resources during resource release and to detect resource abuse or resources being used in unintended or unauthorized manner.
- Security vulnerability management monitoring:
  - Security life cycle management processes should proactively update and patch all deployed software. However, security monitoring systems should look for any missing security patches and report as such to avoid any gaps.

7.1.2 Security Monitoring Techniques

7.1.2.1 Overview

The security monitoring techniques can be classified as:

i) Passive security monitoring;

ii) Active security monitoring; and

iii) Hybrid security monitoring, which are in line with the traditional network monitoring techniques:

1) Passive security monitoring: In this technique, the actual network traffic is captured using various tapping mechanisms (e.g. agent based probing and agentless probing) and the captured telemetric data are sent to the security analytic system to identify the security issues in the network (both virtual and physical).

2) Active security monitoring: In this technique, the additional test traffic is injected into the network along with the normal traffic to identify the vulnerabilities and behavioural status of the network.

3) Hybrid security monitoring: It is the combination of both active and passive security monitoring techniques.

In NFV environment, the physical network elements are running as virtual network functions on virtual machines, so the traditional physical security monitoring systems may not monitor the virtual network functions effectively. Therefore, software based monitoring agents (e.g. virtual TAPs) are needed in NFV environments. Additionally, software based agents also supports rapid scaling and migration features, and are easier to deploy and control than physical probes.Since NFV infrastructure, NFV MANO components, and Network Controllers play a major role in NFV framework, monitoring the virtualised network along with physical network elements is necessary to effectively monitor, detect and deter the security and availability issues.

There are two ways of monitoring the virtualised networks, which are Agentless monitoring and Agent based monitoring.

Agentless Monitoring:

The agentless monitoring on virtualised network is possible through different techniques. For monitoring network traffic, hypervisor knowledge of system resources being used for the traffic destined for certain VNF can be used to monitor that traffic. The challenge here is interpreting the traffic flows into useful results without knowing the application or the semantics in use. Agentless monitoring can also be used directly with VNFs when it is desired not to embed an agent for monitoring.

Agent based Monitoring:

An agent is placed inside the virtual machine to monitor the security aspects of the virtual network function and applications running inside the virtual machine. The agents/probes could be placed along with VNFs in VMs or alone as software agents in separate VMs.

Overview of Security Monitoring Life Cycle:

Figure 10 shows the overview of generic security monitoring life cycle, which consists of the following main stages:

- **Stage 1:** Preparation and collection (injection) of network (test) traffic:
  - This stage deals with the preparation, methods and mechanisms to capture (Inject) the actual network (test) traffic with the guidance of NFV MANO functional blocks and NSM.
  - It deals with where to monitor, what to monitor and how to monitor in the network.
  - It prepares the test agent based on the nature of network traffic that is to be captured and/or security test traffic that is to be injected.
  - It aggregates and classifies the captured telemetry data and sends it for further processing.
- **Stage 2:** Security analytics and detection system:
  - This stage deals with analysing and processing the telemetry data to detect the security issues in the network.
  - Key analytic function of this block can use various big data analytical methods and intelligent algorithms such as advanced machine learning algorithms, etc. to detect the patterns and threat vectors.
  - It deals with the resultant data that could be passed to the next stage to generate alerts and notifications.
- **Stage 3:** Reporting and visualization of analytic results:
  - This stage deals with reporting the analysed results, and generates alerts and notifications to the administrators.
  - It deals with web user interface and graphical statistical results preparation to interpret the analytic results to take further actions.
- **Stage 4:** Decision and security policy enforcement system:
  - This stage deals with how administrators could take actions to mitigate or alleviate the security threats and issues.
  - It deals with the preparation, revision, and enforcement of policies in the virtual and physical network.

The above mentioned stages are not necessarily to be processed in sequential order, for example if the process of stages are automated, stage 3 and stage 4 functions can be processed at the same time in parallel.

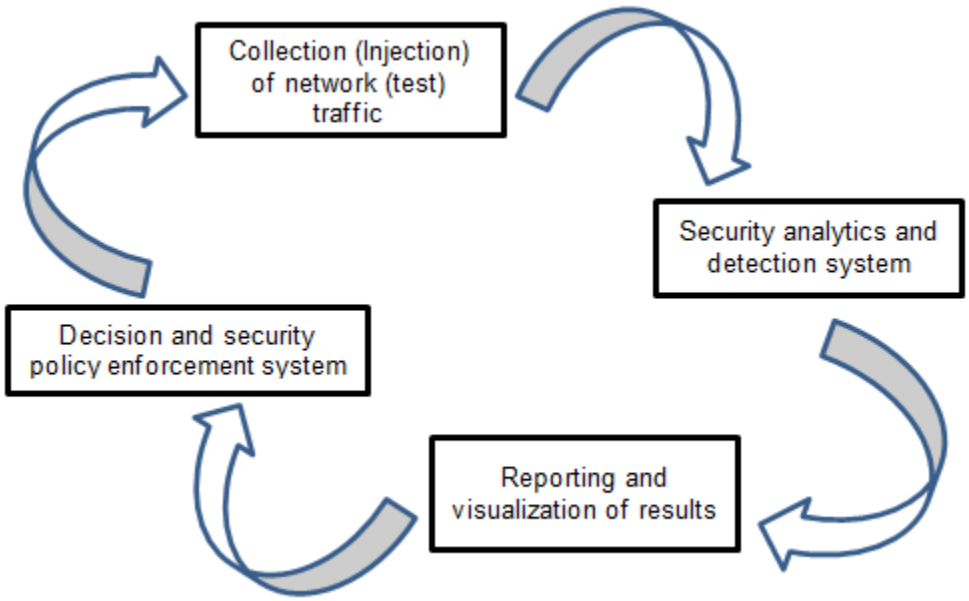

Figure 10: Generic security monitoring life cycle

7.1.2.2 Passive Security Monitoring

Passive security monitoring is a technique that captures the actual network traffic and analyses the captured network parameters to determine the network security and behaviour. The network traffic is collected by using devices like Switched Port Analyser (SPAN), Test Access Port (TAP), network protocol analyser tools and other port mirroring techniques [i.2]. Also it is possible to capture the network traffic at line rate (Gbps) using PCAP, PFQ capturing techniques [i.4]. In NFV systems, Network traffic may be collected and processed for security on the same compute node or across different computes.

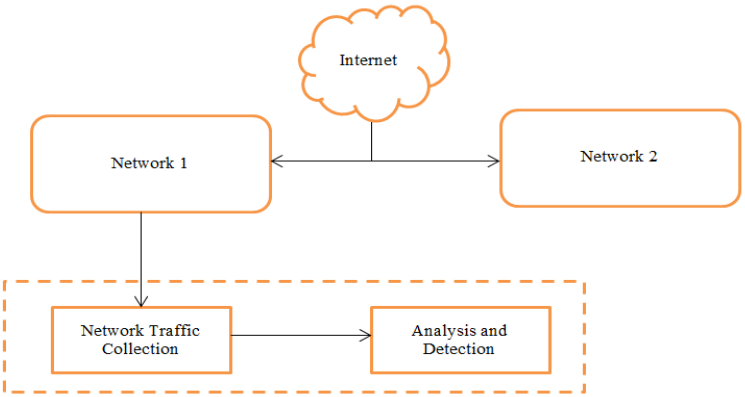

Figure 11: Passive Security Monitoring

Figure 11 shows passive security monitoring technique process, network 1 and 2 consist of various network components like routers, switches, firewall, network intrusion detection system, etc. Network 1 is communicating with network 2 and also getting data from internet. Network traffic is collected from network 1 using various packet capturing techniques and that data is sent to the analysis and detection system for analytic process, where the performance, network behaviour and anomaly detection information will be provided as analysis output results.

Passive security monitoring techniques can be used in different approaches, which are packet level monitoring and flow level monitoring. Packet level monitoring provide detailed information based on the packet traces. Flow level monitoring provide information from packet headers; the flow information contains at least source and destination IP addresses, port numbers, and protocol type information.

It is worthwhile to note that flow monitoring maybe done on actual live traffic without needing to fork off a copy. In this technique, the network flow data from various machines then is collated in a distributed or central manner to detect anomalies using machine learning. The machine learning algorithms may be executed in servers that get the data flow information but are not on the data flow path. Similarly, deep packet analysis may also be done on live traffic.

Analysis and detection system may have deep packet inspection, deep flow inspection, signatures and patterns of anomalies and malicious packets, statistical analysis techniques, etc. to inspect the packets and get the fine-grained information and generate the alerts (like number of detected threats, malicious packet information, suspicious IP addresses, etc.) [i.3]. Passive security monitoring technique can be used to get packet level or flow level information. Based on the thresholds level alerts will be generated and the threshold level defined by administrators.

In case of monitoring the virtualised networks, applications, service function chains, etc., the method of monitoring virtualised entities may vary depending on the deployment model (agent based or agentless monitoring).

EXAMPLE: Hypervisor based agentless monitoring method works only in case of a monolithic operator deployment model.

Similarly, a VNF provider may not agree to embed a monitoring agent from a different vendor necessitating the use of credential based agentless model.

7.1.2.3 Active Security Monitoring

Vulnerable network elements and applications on the network could be exploited by intruders. Active security monitoring can be used to identify the vulnerabilities and patch them proactively. The function of active security monitoring involves:

i) scan the nodes (VMs/VNFs, DBs) for vulnerabilities (unpatched software, etc.);

ii) determining the network topology;

iii) inject the test packets in patterns to assess the actual function/malfunction of the VMs (VNFs) and its applications, and misconfigured ports and services.

Active monitoring framework can be used here for active security monitoring. Software based agents (virtual test agents) can be used to inject the test traffic and collect the responses from the network nodes. In active security monitoring, controlling functionality is handled by NFVO, VNFM, Security Controller and NSM which will give instructions to the test agents on what kind of test traffic to be sent (e.g. what plugins to send) in order to identify the vulnerabilities and availability of network nodes and then will make the necessary decisions to respond to the vulnerabilities learnt through security monitoring.

Use of test packets is mentioned as an illustration. Active security monitoring may also leverage traffic analysers, Intrusion detection and prevention systems when available.

7.1.2.4 Hybrid Security Monitoring

It is the process of utilizing the features of both active and passive security monitoring. Here, active security monitoring technique is used with passive security monitoring to perform the selective monitoring of incoming traffic instead of analysing all the incoming packets. Particularly, active security monitoring can be used to identify the abnormality of particular system behaviour in a network or suspicious packet flows, then that particular node is isolated and passive security can used to do the in-depth security analysis (e.g. DPI). So, hybrid security monitoring can be used to identify and solve the security issues comprehensively.

7.1.3 Limitations and Issues

Limitations

1) Passive security monitoring:

   a) It deals with collected network traffic, so it may help to mitigate the attack reactively but not proactively.

   b) From passive security monitoring point of view, analysing the whole incoming traffic is a huge task and it will delay the decision and security policy reconfiguration process. Also it delays the response time due to telemetry data transit, storage and processing.

c) It may miss many categories of attacks like Web attacks, Integrity attacks, malicious behaviour, propagation of an exploit, etc.

d) End-to-end encrypted traffic does not typically provide much insight in data copying monitoring techniques.

2) Active Security Monitoring:

a) Vulnerability scanners incorporate vulnerability advisories into new set of tests, and there is a time lag between a public advisory of a new vulnerability and the availability of a scanner test for it, and relying on these scanners alone can give a false sense of security during this time period.

b) Vulnerability scanners are complex to use when configuring for a particular target instead of relying on a generic brute force attack profile.

c) Vulnerability scanners don't do a good job of chaining the complex attacks.

3) Agent Based Security Monitoring:

a) Embedding external agents in VNF is a logistical challenge.

b) Agents consume precious resources.

4) Agentless Security Monitoring:

a) Agentless security monitoring takes more time to do the whole process than agent based monitoring approach due to semantic gap.

Issues

1) Passive security monitoring:

a) Passive security monitoring inspects the real network traffic, so there areprivacy issues (invading confidential private information) when inspecting the payload directly.

2) Active security monitoring:

a) The additional test traffic used in active security monitoring consumes network bandwidth and sometimes it may also disrupt the network operations.

3) General:

a) The security monitoring agent may be compromised by attackers and that may be used to gain internal information of the virtual functions.

b) If hypervisor is compromised in agentless monitoring approach, then the total virtual network is under the control of attackers.

c) If the security monitoring controller/orchestrator is compromised, then the whole NFV network environment might be under the control of the attackers.

d) The way of monitoring and processing packets in one domain may be considered as illegal or violation of regulations in another domain.

NOTE: The following use cases refer to Passive Security Monitoring as illustration. Active Security Monitoring could also be applicable.

7.2 Security Monitoring Use Cases

7.2.1 Deployment Scenario: EPC

In an Evolved Packet Core (EPC) environment, using passive probes, one can monitor control plane messages such as GTP-C, S1-C for EPC and SIP control messages for VoLTE, track end-to-end control plane messages for session call creation and termination, etc. These probes can also capture user plane packets such as GTP-U for protocol analysis and deep packet analysis.

Figure 12 shows an example of a few monitoring points in an EPC network for both data (S1U) and control plane (S11).

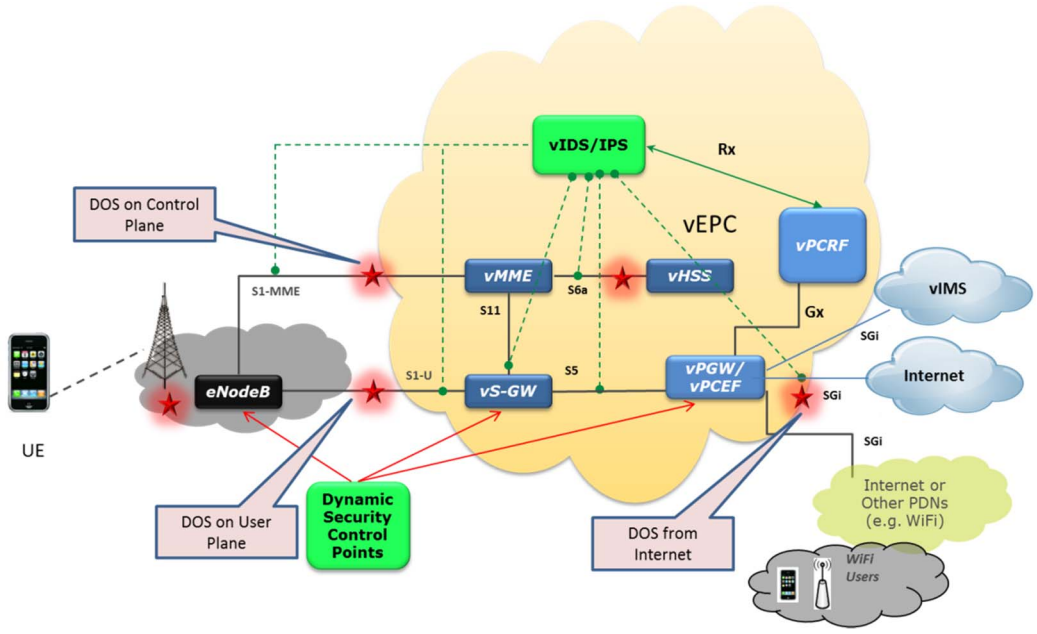

Figure 12: Monitoring Points for EPC Networks

7.2.2 Deployment Scenario: Network Based Malware Detection

The monitoring pertinent to this use case allows network providers to pinpoint and analyse malware in subscribers' home networks and mobile devices. An operator can then take action to protect both the network and subscribers.

As depicted in figure 13, the data are collected by the network-based intrusion detection system (NIDS) over multiple taps. The purpose of NIDS is to detect the malicious traffic originating from the subscriber home network, and to do so it is equipped with traffic-sensing and intrusion-detection software. NIDS is optimized for high bandwidth and flow density, and it is deployed over strategic locations within the network. (In figure 13, traffic is tapped at the *Gn* interface and at the *peering router*.)

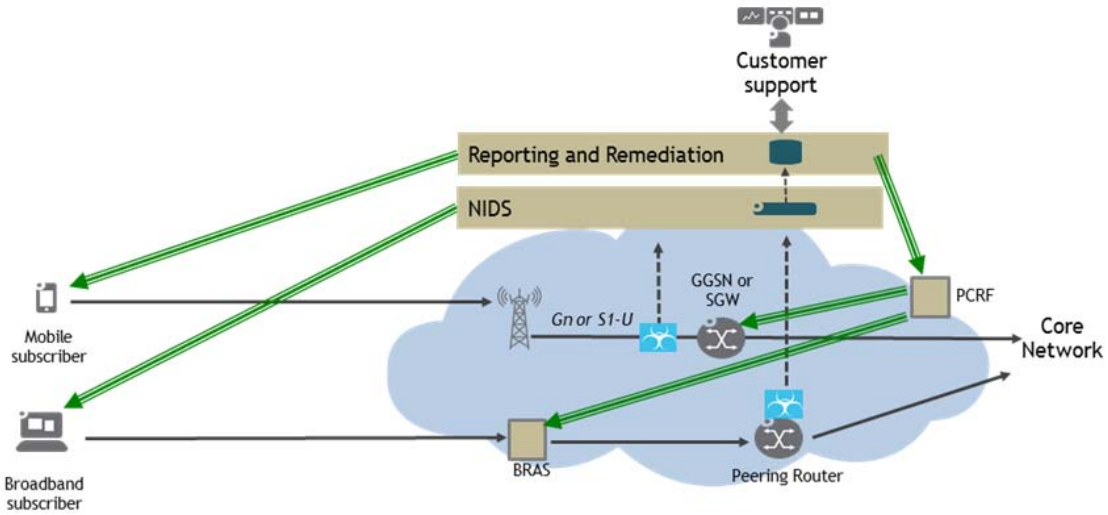

Figure 13: Network-Based Malware Detection, Reporting and Remediation

The traffic is monitored passively using a tap or a mirrored port on a router, producing no negative effect on the network performance. NIDS detects malware-effected behaviours such as command and control communication, backdoor connections, and attempts to infect others. The major thrust is developing insight based on security analytics in addition to having the option to generate subscriber alerts to help eradicate the malware at the source. The NIDS, in conjunction with the reporting function, aggregates and filters the information to correlate among three data sources to derive security insights: subscribers, known malware communication behaviours, and malware's network resource wastage information. The end result then pinpoints the most-infected subscribers, the most-common malware in the network, and the associated resources that are consumed.

The insight established by NIDS is typically provided via a *dashboard*, which also reflects the impact of malware on network bandwidths and signalling.

Reporting and remediation are typically deployed in the service provider's data center, where all respective actions are being taken. The actions vary depending on the provider's policies and procedures.

Integration with the PCRF is an effective means of triggering network actions such as quarantine or blocking. Depending on the type of the subscriber's access, the PCRF instructs BRAS or GGSN or PGW to take an appropriate action.

Another thrust is to address problems effectively at the root. To this end, alerts are sent to infected subscribers providing them with the instructions and tools to remove malware. Integration with customer support allows proactive reaching out to the most-infected subscribers, helping them to remove malware. Alerts and proactive reaching out can also enable value-added services. Continuous detection and elimination of malware can also be offered as a service.

7.2.3 Deployment Scenario: Subscriber Signalling

Monitoring of subscriber signalling (e.g. SIP) for DoS attacks is a well-known use-case, relevant to various types of networks. SIP is an IETF protocol and is used in 3GPP IMS for subscriber signalling, and is handled by multiple IMS functions including P-CSCF, I-CSCF, S-CSCF, MGCF, BGCF, MRFC and AS functions. Monitoring of SIP for attacks can be applicable to other services outside of IMS, and monitoring of signalling can be applicable to signalling protocols other than SIP.

As an illustrative example, SIP servers in general can be particularly vulnerable to semantic denial-of-service attacks, where a client, maliciously or through error, fails to comply with the expected message dialogue sequences - for example by failing to follow up with an expected message, or by sending messages out-of-sequence, or by sending repeated messages. Other examples of denial-of-service attacks can include malformed messages (including very minor perturbations that are difficult to handle with typical SIP parsers), irresolvable URIs and attacks involving authentication attempts. Many variants of these types of attacks can be difficult to detect, such that they impact the servers undetected, or they at least consume resources for a period of time before detection.

Signalling traffic will be monitored using one or more vTAPs. The placement of vTAPs will be chosen based on the placement of virtual network functions that process the signalling traffic - for example, a media gateway control function (MGCF). An alternative architecture would involve logging of signalling traffic by the virtual network function, and monitoring of logs by the analytics function.

Figure 14 illustrates the security monitoring architecture including vTAP and signalling VNFs. In addition to illustrating 'real' VNFs that are providing actual service, the diagram also illustrates the optional use of 'honeypot' VNF instances that are not advertised to genuine subscribers such that any traffic targeted at them is likely to be malicious.

The analytics function employs machine learning and other techniques to detect known and unknown threats. Known threats are recognized through their 'signature' while unknown threats are recognized as anomalous patterns of traffic that deviate from the learned norm. The diagram further illustrates the integration of the security monitoring function (i.e. Security Analytics) with an orchestration function (i.e. Security Autonomics) that undertakes automated mitigation actions to remediate security incidents as they are detected. The actual actions to take are governed by policy, and decisions are enabled by the derived security intelligence provided by the analytics function. Examples of actions could include instantiation of virtual security functions, configuration of security functions (e.g. filtering rules), migration of virtual network functions, enabling of additional levels of monitoring or logging (e.g. for later forensic analysis), etc.

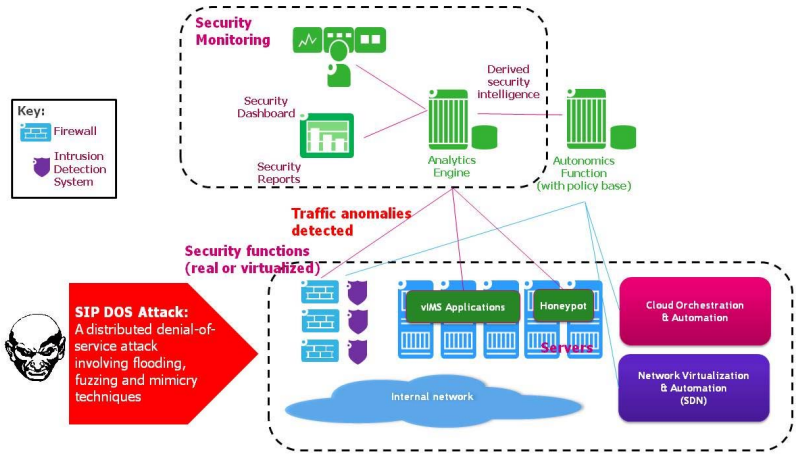

Figure 14: Subscriber Signalling Monitoring

7.2.4 Deployment Scenario: IMS Network Monitoring

7.2.4.1 Overview

IP Multimedia Subsystem (IMS) is an architectural framework, which supports to provide various multimedia services including voice and video over the packet switched network. IMS is an access independent framework; therefore it can support multiple access network types such as GERAN, UTRAN, E-UTRAN, WCDMA, WLAN, Wi-MAX, wire line broadband technologies, and next generation radio networks. Figure 15 shows the simplified IMS architecture with multiple packet switched access networks.

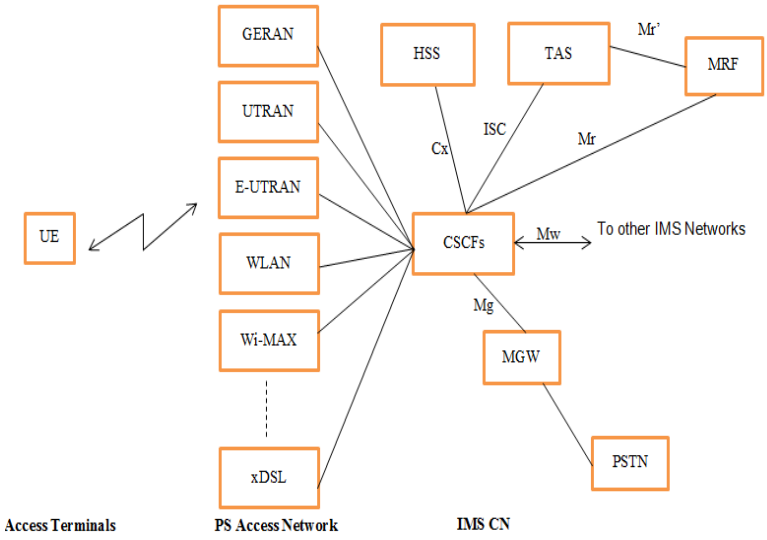

Figure 15: Simplified IMS architecture with multiple PS access network

7.2.4.2 Security Issues

There are several security issues identified in open literature regarding IMS [i.7], such as: Spoofing, identity theft, fraudulent usage of services and resources, session hijacking, DoS/DDoS attacks against network elements (SIP servers, proxies, gateways, and application servers) by exploiting vulnerabilities and sending continuous crafted request message from multiple sources or packet bombarding, call tracking, SQL injection, tearing down sessions, man-in-the-middle attack, registration hijacking, unauthorized access, eavesdropping, social attacks like spam over internet telephony, DNS (ENUM) cache attack, etc. Attackers can utilize these issues to perform attacks depending on the weakness and vulnerability present in the system due to the design, development, deployment, and configuration flaws.

7.2.4.3 Security Monitoring the IMS Core Network

Security Monitoring the IMS network can enable the possibility of detecting the threats and attacks in the early stage to mitigate and reduce the impact of the attacks. In IMS core network, signalling protocol (SIP) and media protocol (like RTP) are used to set up the connections and provide the services respectively. Security monitoring of both protocols (signalling and media plane) are necessary to detect and mitigate the various security issues.

IP Multimedia Core Network (IM CN) subsystem consists of signalling and bearer related network elements to support multimedia services over the IP network. IM CN connected with user equipment's via IP-Connectivity Access Network (IP-CAN), which may be 3GPP based, non-3GPP based, or combination of both the networks. IM CN subsystem supports roaming and interworks with existing fixed and mobile networks, including PSTN, ISDN, packet cable network, and other networks provides IP multimedia sessions and services.

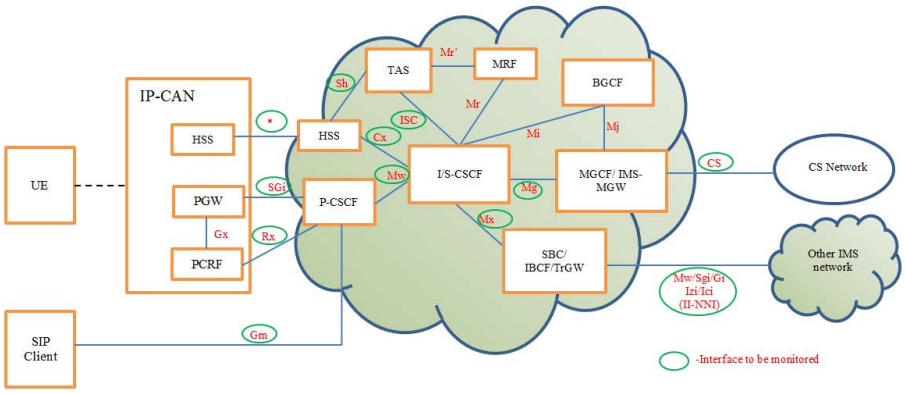

Figure 16: Security Monitoring of IMS network

Figure 16 shows the security monitoring of IMS network [i.7], [i.8]. Following are potential monitoring interfaces [i.9], [i.10], [i.11]:

- Gm interface (PGW - P-CSCF): SIP protocol is used.
- Rx interface (PCRF - P-CSCF): Diameter protocol is used.
- Mw interface (xCSCF - xCSCF): SIP protocol is used.
- Cx interface (xCSCF - HSS): Diameter protocol is used.
- Sh interface (HSS - TAS): Diameter protocol is used.
- ISC interface (S-CSCF - TAS): SIP protocol is used.
- Mg interface (S-CSCF - MGCF): SIP protocol is used.
- Mx interface (I-CSCF - SBC/IBCF/TrGW): SIP protocol is used.

Security Monitoring Agents (SMA) can be placed inside the IMS functions to monitor the particular functions.

In the roaming scenarios, the IMS network is connected with other IMS networks via inter-IMS network to network interface (II-NNI). In that case, additional interfaces (e.g. II-NNI, S9, Mw, Sgi, Gi, Izi, Ici) used for interconnections and transferring information should also be monitored to detect the roaming related security issues.

7.3 Evolving Trends Affecting Security Monitoring

Key trends affecting security monitoring are:

- Stateful and stateless information originating from subscribers and systems need to be identified and recorded in the context of NFV transactions and flows.

- Recorded information may be utilized to represent a range of security needs, which include subscriber information, configuration information, configuration state, etc. all the way to a complete recording of the communication flow.
- Data to be anonymized and excluded from monitoring tools, for privacy reasons, shall be protected against overt usage and re-identification to respect privacy, do-not-track directives and other policies.
- When state information is not provided or cannot be maintained, pseudo-state tokens, parallel session IDs, or other unique GUIDs can be attached to the session and flow data or maintained separately in a database.
- In some deployment scenarios, the VNF(C)-VNF(C) traffic may be protected for confidentiality, as deemed necessary based on the various network conditions, including when the VNFs are communicating over an untrusted network.
- Full end-to-end encrypted data traffic communication for Over-The-Top services is increasingly being deployed. In such scenarios, security monitoring will be limited to control and signalling traffic. Data traffic security monitoring will require additional key management procedures (out of scope of the present document).
- Mobile Edge Computing (MEC), Wireless LAN and 5G technologies are evolving at a fast pace and expected to be one of the critical services delivery mechanisms. Since these deployments are expected to be part of the Operator and Service Provider networks, it is expected that traffic to be monitored. It is expected that the security monitoring techniques illustrated here will be applicable to these, as well.
- The Cloud OS (e.g. Openstack, others) are also now a critical security component which also needs to be monitored for various usages. It is expected that the Security Monitoring solution will correlate to Cloud OS management and control planes.

7.4 Security Monitoring and Management in Virtualised Networks

7.4.1 Security Monitoring As An Infrastructure Capability

Security management requirements for virtualised infrastructure necessitate introduction of a new security management entity that provides secure dynamic delivery of security services into this virtual network. This new security management entity (functional block) may be referred to as 'Security Controller'. It can be mapped to the NSM or ISM defined in clause 6.3, depending on whether it covers the domains in service/tenant layer or the infrastructure layer. Hence there are different types of Security Controller like Tenant's Security Controller and Infrastructure Security Controller. Security Controller is a security component that complements MANO components for NFV deployments security and trust. The Security Controller automates or manually triggers MANO to deploy and/or activate Virtual Security Functions (VSFs) and Infrastructure Security Functions (ISFs), to the NFVI, thus creating a pool of virtual security devices. This is illustrated in the Security Monitoring Architecture.

VSFs and ISFs may be Security Monitoring Agents, Firewalls, Intrusion Detection/Prevent Systems, Anti-Malware, Sandboxes, Security Identity Managers, and Data Loss Prevention, or any other security functions deemed necessary by the security administrator of the NFVI deployment domain, or of the tenant domain. These VSFs may be deployed manually or through an automated policy-driven NSM. Any component within the NFV architecture (e.g. NFVI, VNFs, VNFCs, MANO entities, VMs/Containers, etc.) can be associated with or mapped to the services offered and policies enforced by these VSFs. VSFs and ISFs will be collectively referred to as a generic term, Security Services Agent (SSA), in the present document and is defined in the Security Monitoring Architecture, clause 7.6.

The Security Controller oversees the assignment of slices from those VSF pools to components defined by the NFV architecture. SSA can be treated as a VNF for purpose of NFV architectural consistency, and can be instantiated within the NFVI (e.g. within hypervisor, network devices like LAN or switches, etc.) for NFVI domain, or by the tenants as their VNFs/VNFCs in their respective virtualised tenant domains. A Security Controller may be limited in its visibility and ability to influence multiple trust domains, in which case it limits itself to the trust domain that it can establish trust with.

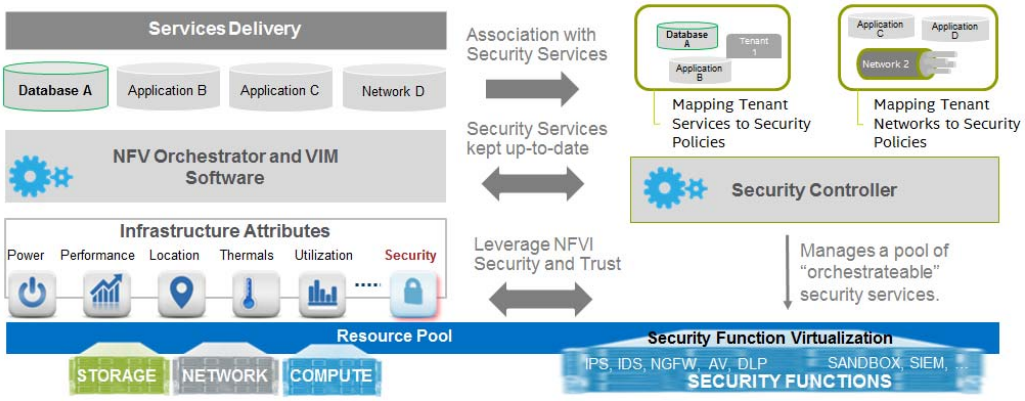

Figure 17: Security Monitoring As An Infrastructure Capability

A Security Services Agent will be associated with its VNFM and EM. After secure instantiation and bootstrapping, a SSA will connect to its VNFM and EM for receiving configuration, policy and any associated data (e.g. signatures for Malware, etc.). The initial basic SSA configuration may be done by VNFM, and SSA application level configuration by its Element Manager. All SSAs are treated consistently so no matter which VSF or ISF performs security monitoring of a certain type, it leads to a uniform result as defined by the trust domain-wide policy.

An Infrastructure Security Controller will manage multiple Security Monitoring Agents, like ISFs that are deployed across multiple physical hosts within a NFVI, and on physical hosts across distributed NFVIs. Likewise, a Tenant's Security Controller will manage multiple Security Monitoring Agents, like VSFs, that are deployed by the Tenants as their VNFs. There is a clear security monitoring policy and enforcement separation and independence (mutually exclusivity) between various trust domains.

7.4.2 Data Access in Virtualised Environments

There can be different forms of virtual tap (vTap) and virtual Front-End Processor(s) (vFEP) based on the NFV deployments in the network. These could serve as selective-filtering or splicer role, and in some case, might also be part of the service function chain. Whenever a new VNF is instantiated, the MANO infrastructure shall inform the security controller so the security controller can decide to trigger the instantiation of an SSA if required. Positioning of SSAs will be dependent on a variety of factors, and requires significant knowledge of the existing, current network topology. When these are part of a VNF, then they are instantiated as part of the normal instantiation procedure, and then there shall be a process whereby they become known to the security controller, and is defined in the VNF Bootstrapping protocol clause in the present document.

7.4.3 Non Standard Interfaces

Some VNFs do not use any standards (e.g. 3GPP) specific protocol for inter communication but use either vendor proprietary protocols or use shared memory or local database to communicate in order to optimize the inter VNF communication. These systems expose the standard interfaces only when their systems need to interoperate with another vendor component.

EXAMPLE: Some of the vEPC vendors use non-standard interfaces for the communication between MME and HSS instead of standard diameter-based S6a interface, but exposes diameter interface while talking to external HSS. In some cases, they use optimized protocols in order to reduce the signalling overhead.

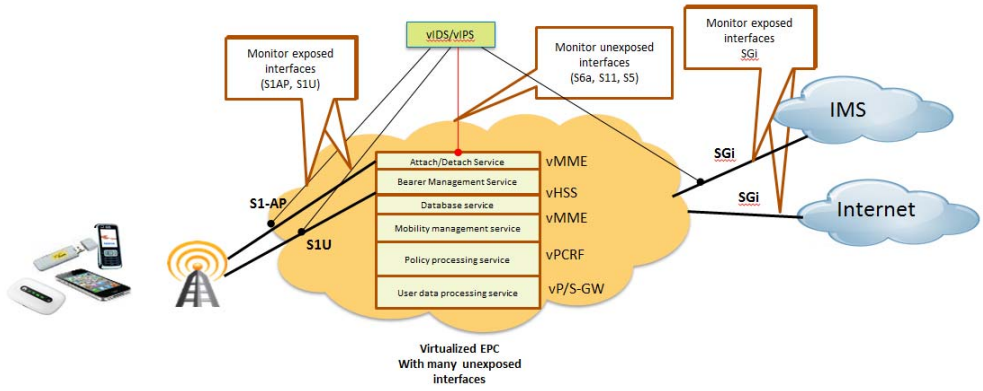

Figure 18: Non-Standard Interfaces

In such scenarios, it would be difficult using the normal vTap to gather both control and data packets to provide any analytics or detect any specific anomaly in the network. In these situations, the vendors will need to expose their APIs directly to vFEP to "bring it back to the more normalized form in 3GPP" or via Element Management System (EMS) or by some other means they will need to provide the required Meta data in a timely fashion to feed the vFEP. Push/pull mechanism or subscribe/notify mechanism can be implemented to notify the related control and data information to vFEP.

7.4.4 Monitoring ETSI-NFV Defined Interfaces

ETSI NFV has defined an architecture in ETSI GS NFV 002 [i.6]. Based on the ETSI NFV architecture, five-level security monitoring should be implemented across the ETSI NFV architectural components and Reference Points, which are described below:

- Physical resource monitoring: It is to monitor the physical resources, including physical computing, physical storage and physical network. The NFV SSAs used for physical resource monitoring send the telemetry data to NFV SSP in VIM for further analysis. This is part of the NFVI administrative domain.
- Virtualised resource monitoring: It is to monitor the virtualised resources, including virtual computing, virtual storage and virtual network. The NFV SSAs used for virtualised resource monitoring send the telemetry data to NFV SSP in VIM for further analysis. This is part of the NFVI domain.
- VNF-level monitoring: It is implemented within a VNFC to monitor other VNFCs in the same VNF for a Tenant. The NFV SSAs used for VNF-level monitoring send the telemetry data to NFV SSP in VNFM for further analysis. The VNFC level monitoring is part of a Tenant's administrative domain.
- NS-level monitoring: It is implemented as a separated VNF to monitor other VNFs in the same NS. The NFV SSAs used for NS-level monitoring send the telemetry data to monitoring tools. The NS level monitoring is part of a Tenant's domain.
- System-level monitoring: It is to monitor the system wide security based on the NS-level telemetry data received from the corresponding NFV SSAs, as well as the physical resource telemetry data, the virtualised resource telemetry data and the VNF-level telemetry data individually received from NFV SSPs in VIM and VNFM. It is able to analyse and handle telemetry data from different networks and tenants to deal with cross-domain security problems. This level of monitoring is only possible when both the Infrastructure provider and the Tenants agree to participate in such a scheme that spans multiple trust domains.

These security monitoring levels are articulated in the Security Monitoring Architecture described in the subsequent clauses.

7.5 NFV Security Monitoring & Management Requirements

7.5.1 Overview

Security Monitoring & Management of a NFV system is a methodology and diligent process that spans the complete life-cycle of the virtualised system. At any point of the system state, it should be possible for the NFVI administrator to ascertain the security health of the entire NFV system. A trusted Security Monitoring & Management system is necessary for secure deployments of NFV. These requirements and deployment guidelines apply to the VNFs and/or VMs behaviour and network traffic in the NFVI.

Security Monitoring & Management builds upon certain security pre-requisites that have been discussed in the ETSI NFV Security and Trust Document [1], including addressing critical security areas identified in the ETSI NFV Security Problem Statement [2].

7.5.2 Security Hardening Requirements

Generic security requirements for a security monitoring solution in the NFV environment include:

S1 Network monitoring solution shall not render vulnerable the security of the network or the user data any more than it is without the network monitoring solution in place.

S2 The monitoring solution in NFV shall provide an equivalent or higher level of security than the monitoring solutions in existing non-virtualised networks.

S3 Active Monitoring failures should be fail safe. Passive monitoring failures should be silent from user perspective.

S4 The Security Monitoring components should be protected from other NFV system components, and should execute in Hardware Mediated Execution Enclave (HMEE) within appropriate trust domains.

S5 Security Monitoring should not impact IAAS, PAAS, and SAAS SLAs.

S6 Security Monitoring depends upon security requirements established by the ETSI GS NFV-SEC 001 [1], including Secure and Measured boot and establishing secure channels based on mutual authentication.

S7 A comprehensive deployment of Security Monitoring solution will monitor both virtualised and non-virtualised network functions.

S8 NFVI resource allocation and platform quality of service technologies should be put in place to ensure that the Security Monitoring functions are not starved of NFVI resources causing unexpected security consequences. Such mechanisms should reliably ensure that Starvation and DoS attacks against Security Monitoring functions are minimized or eliminated.

7.5.3 Securely Provisioning Security Monitoring Components

Security Monitoring is a set of services and needs to follow strict security principles for operational use:

S9 Security Monitoring components shall be securely provisioned within the system, which means that these systems will be provisioned for deployments in a trusted environment. This includes root key provisioning, setting up HMEE, certificate provisioning, etc.

S10 Security Monitoring components shall be booted using secured and Measured boot technologies.

S11 Once Security Monitoring and Management systems are in place, these shall detect authorized and unauthorized on-boarding, deployments, activation, and run time integrity checking of VNFs.

S12 Once VNFs are deployed, Security Monitoring and Management System shall ensure that the security policies of the deployed VNFs are enforced.

7.5.4 Secure Telemetry Access For Security Monitoring

Trusted access to Telemetry will form the backbone of any Security Monitoring system. Telemetry will be a crucial input upon which the Security Monitoring will depend for delivering dependable insights into the NFV system. It is expected that the Telemetry will facilitate detection of security anomalies within the system, and in advanced usages, analytically use telemetry patterns to predict emergence of security threats:

S13 Telemetry security policies for Security Monitoring of the NFVI will be established by the NFVI administrators.

S14 Telemetry will include collection of data across various physical and virtual components in the NFV system, and do this in a dependable manner. Telemetry includes NFVI system configurations, policies, network traffic content, packet headers, etc.

S15 Telemetry will be securely delivered to the Security Monitoring Systems, as per the Security policies.

S16 Security Monitoring Telemetry can include sensitive materials and might be subject to additional Data security policies and authorized access. This includes telemetry source and destination authentication, telemetry data integrity and confidentiality, opportunistic encryption, trusted time, and synchronization across multiple NFVI systems.

S17 Security Monitoring systems shall protect Telemetry data-at-rest, both at local or remote secure storage.

S18 Security Monitoring telemetry may be compressed prior to storage and/or during transit.

7.5.5 Monitoring VNFs and Service Function Chains

Security Monitoring will enable active and passive monitoring of the VNFs and the Service Function Chains (SFC) which have been provisioned in the NFV environment. Monitoring and remediation will follow defined security policies. In cases when these requirements are violated, appropriate countermeasures and remediation will be deployed, which include, but not limited to, blocking VNF instantiation, killing malformed configurations, blocking SFC traffic, sending traffic for further analysis, etc. The NFV administrators are expected to create and maintain an exhaustive list of remediation and countermeasures, and deploy those in a timely manner, whether automated or manually:

S19 A Security Monitoring and Management system will ensure that the VNFs and SFCs have been securely configured, meaning that start-up and security enforcement policies (e.g. VNFDs, Configuration) were delivered to the VNFs in a protected manner. It is assumed that the configuration data itself is vetted and accurate, per the security policy.

S20 Once provisioned, Security Monitoring and Management system will ensure that the VNFs are not activated unless their security policy is addressed. For example: all VNFs in a SFC should be deployed prior to activation of a specific VNF.

S21 The Security Monitoring and Management system will facilitate that a SFC topology is verified, and is securely activated.

S22 The Security Monitoring and Management system will help monitor VNF topology changes, including migration, scale-in, and scale-out of VNFs.

S23 Security Monitoring and Management will observe the VNFs creation and termination process and it should be able to detect and remediate improperly authorized actions.

S24 The Security Monitoring and Management system will help detect and remediate VNF exploits during the normal course of VNF's operational life-cycle. For instance, attacker could attempt to exploit a known vulnerability in a VNF, which can be detected and blocked by the security monitoring system.

7.5.6 Orchestrating Security Monitoring As A Service

Security Monitoring can be considered a privileged set of security services that have policy controlled access to the NFV system components:

S25 As with any other NFV service, the Security Monitoring services will also be orchestrated.

S26 NFV Security Monitoring components should run in a HMEE.

S27 The NFV Security Monitoring and Management system shall ensure that all Security Monitoring services and policies are securely provisioned and activated prior to NFV system bring-up.

S28 NFV Security Monitoring and Management system shall interface with the NFV system life-cycle, including hardware, firmware, and software updates, to ensure that these are authorized and occur per security policy.

S29 Security Monitoring may perform Active and Passive Security Monitoring of the Control, Management, and Data planes in a VNF.

S30 Security Monitoring can be continuous, manual, or triggered by a specific set of events, as in automated anomaly detection. Monitoring can also be triggered by an administrator based on their specific criteria.

S31 NFV Security Monitoring system may securely distribute telemetry to multiple Security Monitoring Collection and Analytics Systems, based on the security policies for minimizing latencies associated with detection remediation of threats.

7.5.7 Securely Auditing Security Monitoring

Security Monitoring services should be designed to be inspected for adherence to security controls, policies and procedures:

S32 Security Monitoring components should follow security best practices for auditing, including secure logging and tracing.

S33 Audit logs contain sensitive information, and based on security policy, Audit Log data-at-rest should be confidentiality and/or integrity protected with a securely provisioned key.

S34 The Audit Logs, in transit, should be integrity and confidentiality protected using pairwise unique keys.

7.5.8 Operational Requirements

Security Monitoring services should be designed to address operational criteria and procedures:

S35 Network Monitoring should not lower the reliability of the system from its state prior to enabling Security Monitoring.

7.6 Security Monitoring and Management Architecture

7.6.1 Overview

A Security Monitoring and Management system will comprise multiple components, which can be distributed across the NFV system, and be used for affecting a broad range of deployment-specific monitoring. Each deployed NFV system will have its unique set of Security Monitoring requirements, and these requirements may even vary within the same NFV deployment for each tenant, service, flow, or any other Infrastructure owner defined criteria.

This clause will discuss System Monitoring and Management architecture. This architecture enables a broad understanding of the system security design, without specifying or mandating any specific implementation.

7.6.2 Architecture Constructs

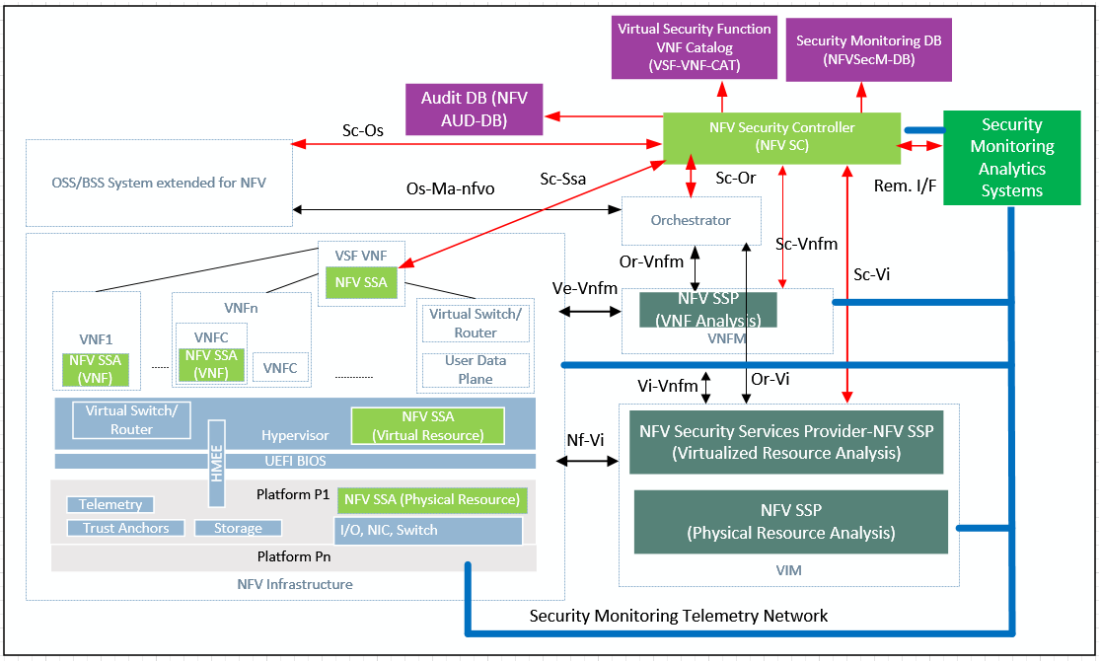

Figure 19: NFV Security Monitoring and Management Architecture

Figure 19 describes the NFV Security Monitoring and Management architecture. This logical architecture comprises of the following components, each of which comprises APIs and functions. In specific implementations, as determined by trust domains and deployment security policies, a particular instance of a Security Controller may have one or more of the reference points shown in the diagram, but may not necessarily implement more than one reference point. This security model builds upon the ETSI NFV architecture, and proposes security enhancements to the ETSI NFV architecture:

- NFV Security Services Agent (NFV SSA):
  - The NFV SSA exists in both the NFVI domain and in VNF domain. NFV SSA in VNF domain may exist as a separate VSF, or within a VNF. The NFV SSA is responsible for securely receiving the Security Monitoring policy and implementing the same.
- NFV Security Services Provider (NFV SSP):
  - The NFV SSP is comprised within the VIM and VNFM, and is responsible for security monitoring policy orchestration received from the Security Controller (NFV SC) and interacting with the various VIM/VNFM components to implement the policy across various systems comprising the NFVI/VNF. Furthermore, NFV SSP is also responsible for receiving the telemetry data from various NFV SSAs, and optionally making some analysis based on this data.
- NFV Security Controller (NFV SC):
  - The NFV SC may interface with other security systems (e.g. Security Analytics), security databases and other policy engines. The NFV SC orchestrates system wide security policies. The NFV SC acts as a trusted 3rd party that resides independently. An NFV SC manages NFV SSAs (like VSFs) to keep them in a consistent state according to the policy specified. NFV SC includes a SSA catalog of security functions that can be orchestrated and deployed at system start-up or dynamically using the VIM, and SC also facilitates secure bootstrapping of SSAs (like VSFs), managing instances of SSAs, secure pairing up with SSA's VNFMs and EMs, personalize the SSAs, policy management, integrity assertion, credential management, facilitate clustering of multiple SSAs into a distributed appliance, monitoring of SSAs for failure and remediation. These functions and protocols are described in subsequent chapters.

- NFV Security Monitoring Analytics System:
  - The NFV Security Monitoring Analytics system comprises of functionality that performs secure Telemetry acquisition from the NFV system, and can derive threats and anomalies from the telemetry, and expected to initiate security countermeasures and remediation.

The functionality of each of these components should be implemented within a HMEE, with every instantiation identified by its globally unique instance identifier. Unique instance identifier ensures distinct security identity for each instance useful for security protocols endpoints identification, auditability, controls, debug, and others secure system wide capabilities are tracking.

The Security Monitoring and Management system comprises of the following logical databases:

- NFV Security Monitoring Database (NFV SecM-DB):
  - The NFV SecM-DB is a secure database consisting of security data used for deploying NFV system wide Security Monitoring. This includes Security Monitoring policy and configurations, security credentials for facilitating secure communications between the various Security Monitoring components, and credentials for secure storage of telemetry, including tenant-specific security policies.
- SSA/VSF Catalog Database (VSF-VNF-CAT):
  - The NFV VSF-VNF-CAT is a repository for Security Services Agents like the Virtual Security Functions (VSF) VNFs. The catalog has capability to add and remove SSAs (VSF) packages and/or images, and also includes a VSF VNFD containing meta data and information about that VSF VNF. Once the SSA (VSF) package or instance is added to the catalog, it becomes available for orchestration.
- The Audit Database (NFV AUD-DB):
  - The NFV AUD-DB is a secure database consisting of security audit information.

The Security Monitoring Analytics system securely receives Security Monitoring telemetry from across the NFV systems, including the MANO and all the NFVIs that may be geographically distributed. The analytics system applies advanced machine learning techniques on the telemetry to perform advanced detection of security anomalies and emerging threats in the system. This system also can trigger remediation actions through the NFV SC.

The interfaces between these various components (figure 19) will use or extend the interfaces defined by ETSI NFV as necessary for Security Monitoring. When possible, existing interfaces extensions (shown in black) will be used. The new NFV Security Monitoring systems interfaces are shown in Red.

There is a Security Monitoring Telemetry Network (shown in Blue), which is used for transmitting protected security monitoring telemetry and traffic (comprising Control, Management and Data packets) from various Security Monitoring Agents to the Security Monitoring Analytics System. This Secure channel will be established using the Security Controller as the trusted 3rd party.

7.6.3 Security Monitoring System High-Level Flows

This clause describes an end-to-end automated Security Monitoring Management system workflow, which can be dynamically executed without user intervention. This is described in figure 20.

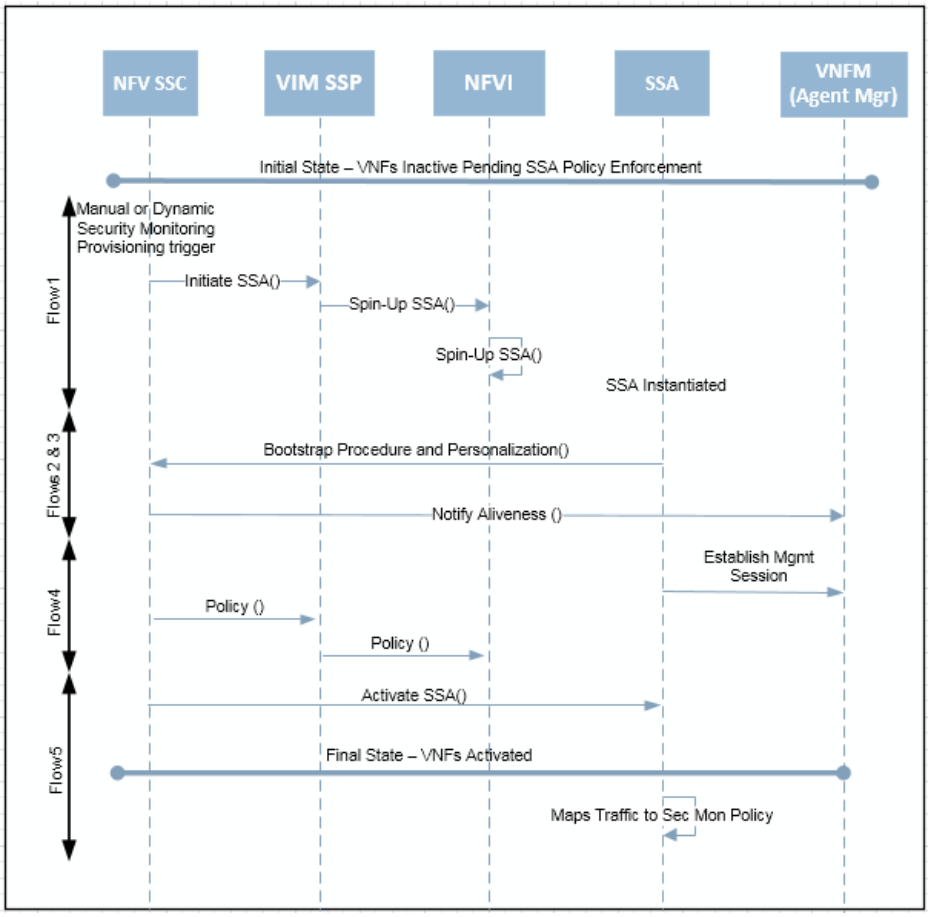

Figure 20: Security Monitoring System High Level Flows

Figure 20 illustrates high level functional flows, as textually described as Flows 1-5 below. Figure 20 does not describe specific implementation messages or control signals, rather a sequence of functional events for provisioning, deploying and activating Security Monitoring.

Flow 1: Secure Provisioning of Security Monitoring:

- The choice between pre-provisioning security monitoring and dynamic/automated provisioning of Security Monitoring is presented to the security administrator. If pre-provisioning security monitoring is chosen as the infrastructure policy, then the SSAs are deployed as part of the NFVI. SSAs can also be dynamically provisioned, in which case SSAs like VSF VNFs are deployed in a scale in/out manner. VIM deploys and instantiates various SSAs on NFVI and within MANO. SSA Security Monitoring options (e.g. VSF like IDS, IPS, Firewall, DLP, Security Monitoring Agents, Telemetry Collectors, etc.) will be presented in the NFV Security controller. Deployment policies may also dictate specific types and numbers of instances of SSAs (VSFs) to be pre-provisioned or dynamically deployed into the infrastructure. The NFV SC validates and performs runtime monitoring to ensure that all the SSAs incl. the VSF VNFs are deployed, instantiated and activated per policy.

Flow 2: Seeding information upon security function Start-up:

- Prior to the booting of security functions, the appropriate security and policy configuration information (e.g. which VNFM and EMs to connect to) will be seeded into the Security Services Agent (say, in the Hypervisor) by the NFV Security Controller. Once the VNFI is running, the seeded data is extracted, the SSA (VSF) executes the secure bootstrapping protocol, and then securely acquires security credentials which are then and used by the SSA for connecting to its corresponding VNFMs and EMs.

Flow 3: Personalization:

- NFV Security Services Agents will each perform secure protocol exchange with the Security Controller to enable each SSA to establish secure connections with their respective VNFMs and EMs which have secure access to the personalization data The VNFM and EM will personalize their Security Services Agent(s), for instance, performing set name, security policy groups, per-tenant policies, and any additional configuration parameters and necessary state information.

Flow 4: Policy Definition:

- On the Security Controller, policy associations between VNFs and SSAs (VSF VNFs) are provisioned, for instance when tenants or new services (VNFs) are provisioned. Tenant VNFs can be put into groups based on various criteria and those groups can be assigned services exposed by SSAs security monitoring devices. The SEM can then push down security policy associated with the VNFs groups to the SSAs. These policies that are then propagated across all SSA's (incl. VSFs). This enables a set of SSAs to apply the security functions policies uniformly across the NFV deployment, no matter which SSA processes that data, management and/or control traffic.

Flow 5: Mapping traffic to security policy:

- The NFV Security Services Agent may interact with the virtual switch and the physical network infrastructure to translate that mapping of VNF group to policy before handing off traffic to the security monitoring SSA. A VNF group may be based on traffic type (e.g. VLAN, MPLS, GTP, etc.) and their associated security policies that will be enforced by the SSA. These mapping may change due to any number of reasons including new tenants joining, tenants leaving, traffic engineering, workload balancing, etc. When this happens, the OSS/BSS system conveys these changes to the NFV SC, which then automates the distribution of the new policy to the SSAs (e.g. in the VSF VNFs).

If the health of the SSA incl. the VSF VNF instance, turns bad, the NFV SC will be responsible for remediating this situation. One option could be to perform runtime inspection of SSAs, and/or terminate and create a new VSF VNFs. SSAs can provide failure detection and remediation options, so that remedy can be made configurable and automated.

7.6.4 Secure VNF Bootstrapping Protocol

When a VNF, including a Security Monitoring SSA or VSF is instantiated on an NFVI, the VNF needs to be securely bootstrapped with its VNF manager and/or its EM. This problem is also discussed in ETSI GS NFV-SEC 001 [1] and ETSI GS NFV-SEC 003 [2].

This clause describes a secure bootstrapping protocol that can be used for the following usages:

- Dynamically creating an initial VNF security credential(s), also known as the root credential(s).
- Addresses VNF Migration and Scale Out of VNFs/VNFCs, where each entity can get its own distinct credential. Based on policy, multiple VNFs may be able to use the same credential.
- Used as the basis for VNF policy validation, including licenses and whitelisting checks. It can be used for securely receiving startup policies, configuration information, and registering itself as an operational VNF.
- Securely identify, then, connect to its VNFM and/or EM. Since the VNF is securely bootstrapped with its manager, the VNF root credential established by this process can be used to derive additional set of credentials for various VNF life-cycle usages e.g. secure communications, policy delivery, etc.
- If for any reason, including administrative checks, the VNF is required to re-issue its root credential.
- Dynamic runtime attestation of the VNF parameters and platform authorization in situations where the VNFI policies might change and require all VNFs to re-authenticate to their managers.

Figure 21 illustrates the block diagram of the entities involved in the protocol execution, in the context of the ETSI NFV architecture.

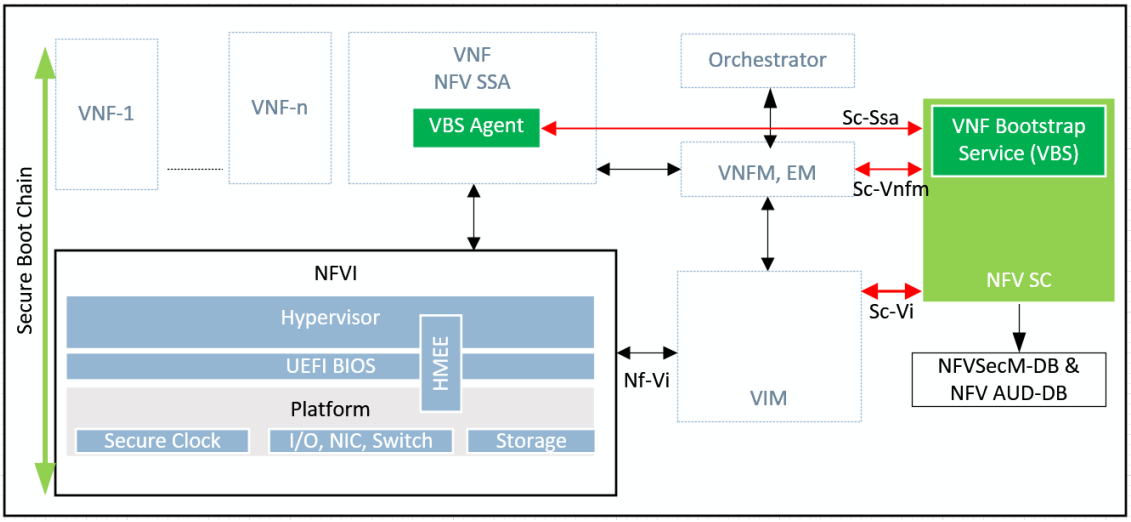

Figure 21: Secure Bootstrapping Protocol Block Diagram

It is assumed that the NFVI and the MANO platforms followed a secure boot process, and that the secure boot chain of trust extends to the VNFs. Also, that the NFVI has hardware-mediated execution enclaves. Hardware-mediated execution enclaves refers to a generic secure execution environment, and has no connection to TEE or SE specified by Global Platform (GP). This hardware-mediated execution enclave (HMEE) has been securely bootstrapped with the NFV Security Controller. HMEE is described in ETSI GR NFV-SEC 009 [i.13].

The main entities for this protocol include:

1) VNF Bootstrapping Service (VBS): The VBS is contained within the NFV Security Controller. The VBS is responsible for managing the bootstrap process from the trust anchor perspective. There might be one or more VBS in the system.

2) VBS Agent: This is the component within the VNF. Each VNF (incl. the Security Monitoring VNFs and SSA) will contain a VBS Agent, which will be responsible for performing the functions and messages required for securely bootstrapping the VNF.

3) A hardware- mediated execution enclave (HMEE): This protocol does not define a HMEE. A platform HMEE can be an independent security engine, an exclusive CPU/Memory mode, or an enclave providing memory encryption and code/data execution isolation.

Figure 22 describes the system functional flows that would be executed within the ETSI NFV defined components. This flow begins prior to the VNF (or, SSA) being instantiated, or when a VNF has been instantiated but not active, when a VNF needs to be securely bootstrapped with its VNFM and then with its EM, or when explicitly desired by the VNFM or EM for runtime attestation of the platform. There might be additional cases in which this protocol can be executed.

This protocol relies on the trust guarantees of the following:

1) That the NFVI and MANO components followed the secure boot process.

2) The HMEE within each NFVI platform has been securely bootstrapped with the VBS.

3) The VBS and the VNFM/EM have been securely bootstrapped.

4) These security protocols defined herein, like any others, rely on unique system wide identifiers for every element of the protocol endpoints. These identifiers may be uniquely generated by an RNG, may be manually assigned, or use random GUIDs.

Further details of steps 2 and 3 are not defined in this protocol, but are assumed to be responsibilities of the system and security administrators. The offline bootstrapping allows for enforcing the policy checks required in this protocol.

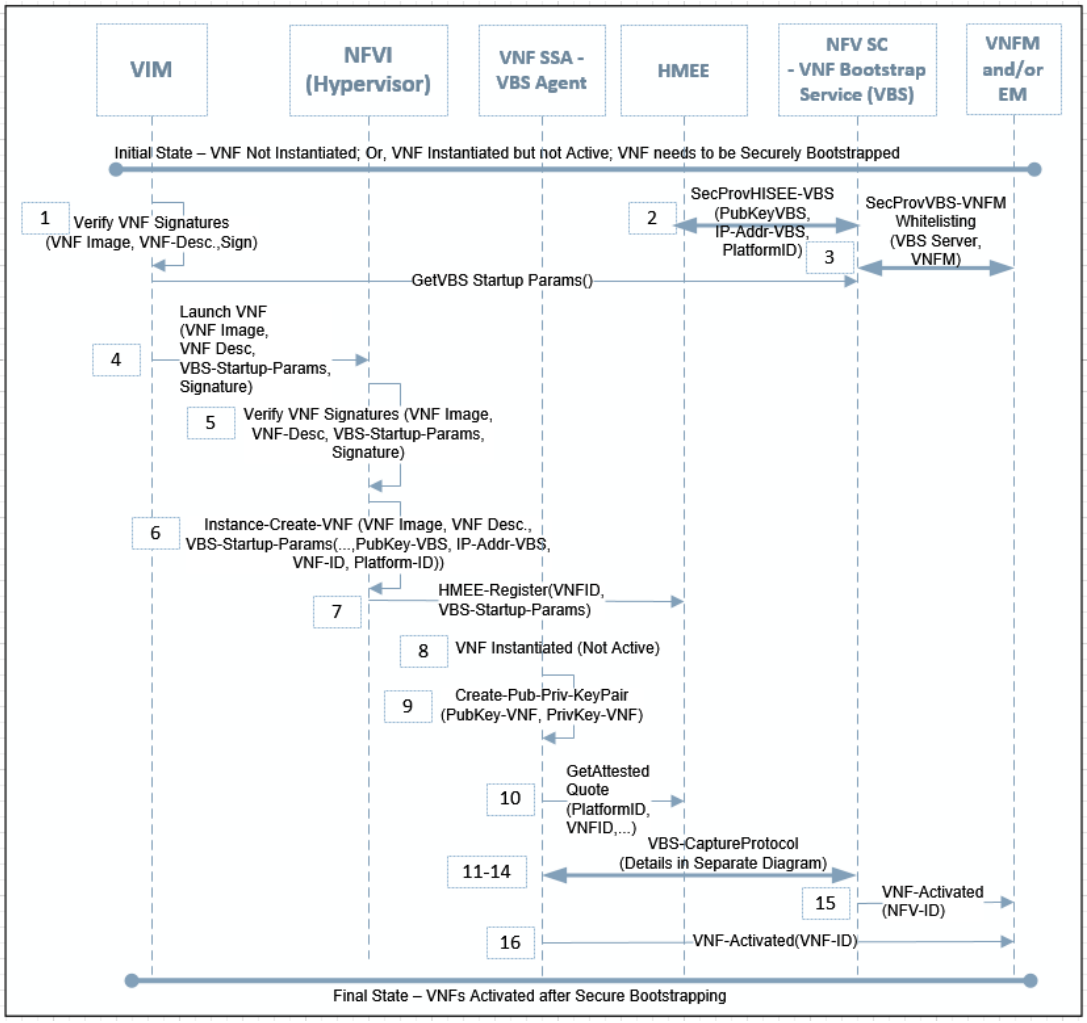

Figure 22: Secure Bootstrapping Protocol System Functional Flow

The VIM verifies the VNF images when the VNF is delivered into the MANO. At the time, the VIM gets the VNF start-up parameters from the VBS, or these might be pre-configured into the VIM sub-system. The VIM initiates a launch with the NFVI, which will again verify the VNF Image, VNF Descriptor, and the VBS startup parameters for the VNF. These startup parameters might be separate or combined within the VNF Descriptor.

Security Monitoring VNF descriptors comprise of tags that define security requirements. As such a NFV SC will need to be notified if the VNF descriptors change, since the SC defines the Security Groups and forms association of VNF descriptors to Security Groups. This defines the VNF's Security Group membership. VNF descriptors also make Security Group memberships dynamic and as the descriptors change, a VNF could change group membership. Each Security Group can have a Security Policy bound to it, which also defines the virtual security monitoring control to be inserted. Since the NFV SSC is notified about changes on those descriptors it would then run the necessary Security Monitoring provisioning steps, including this Secure Bootstrap protocol.

The NFVI instantiates the VNFs with the VBS startup parameters, which include:

- VBS Public Key;
- IP address of the VBS;
- VNF-ID which is a unique system-wide identifier for each VNF; and
- Platform-ID which is a unique system-wide identifier for each platform.

The NFVI Hypervisor also registers these startup parameters with the platform HMEE. At this stage, the VNF is instantiated but not Active. The VBS Agent in the VNF/SSA is initiated which generates a VNF Public/Private key pair. The VBA Agent requests the platform HMEE with an attested quote, which is signed by the Private Key of the HMEE. The VBS Agent then executes the VBS Capture Protocol with the VBS, and upon successful completion of all the steps, initiates the VNF.

The procedure for the HMEE to generate the signed Quote is described as follows:

1) Hashes generated by HMEE based on the inputs into HMEE:

   i) hash-h1 = Hash(VNF-Image, VNF-Descriptor, VNF-ID, Platform-ID), where:

      - VNF-Image is the image of the VNF.
      - VNF-Descriptor is the descriptor associated with the VNF-Image.
      - VNF-ID is the unique global identifier of the VNF instance.
      - Platform-ID is the unique global id. Of the Platform on which the VNF will be activated.

   ii) hash-h3 = Hash (hash-h1, PubKey-VNF), where:

      - PubKey-VNF indicates the key used by the VBS Agent for signing.

2) Hash value independently calculated by HMEE from Secure OOB Provisioning step:

   i) hash-h2 = hash(PubKey-VBS, IPAddress-VBS, VNF-ID, Platform-ID), where:

      - PubKey-VBS, IPAddress-VBS identifies the VBS involved in the Bootstrap protocol.
      - VNF-ID and Platform-ID are as defined in (1).

3) HMEE calculates the Quote hash, then signs the hash by its the Private Key:

   - Quote-Q = [Hash (hash-h2, hash-h3)] PrivKey-HMEE.

Analysis of the HMEE Quote:

- The VNF-IDs allow multiple instances of the same VNF-Image to be instantiated on the same platform.
- Platform-ID identifies the platform on which the VNF instance will be activated.
- The HMEE binds the VNF Image, VNF Descriptor, VNF Instance, Platform, VBS, and VNF Public Key.
- The secure provisioning of the HMEE with the VBS, and the VBS with the VNFM and the EM is essential to hold the security properties of this protocol.
- This protocol is optimized for performance, but can be made tighter by including hashes into subsequent hash and signing operations.

The Secure Capture protocol is described in the figure 23. The Capture protocol is a 4-way handshake that enables secure binding of the VNF (VBS Agent) with the VBS. As mentioned earlier, the VNF can be a Security Monitoring SSA, VSF or any VNF, VNFC, or VM. The security properties offered by this 4-way handshake include: Session separation, session liveness, protocol freshness, replay protection, integrity protected handshake, protection from masquerading attacks, MITM protection, and whitelist checking based on the security policy of the deployments.

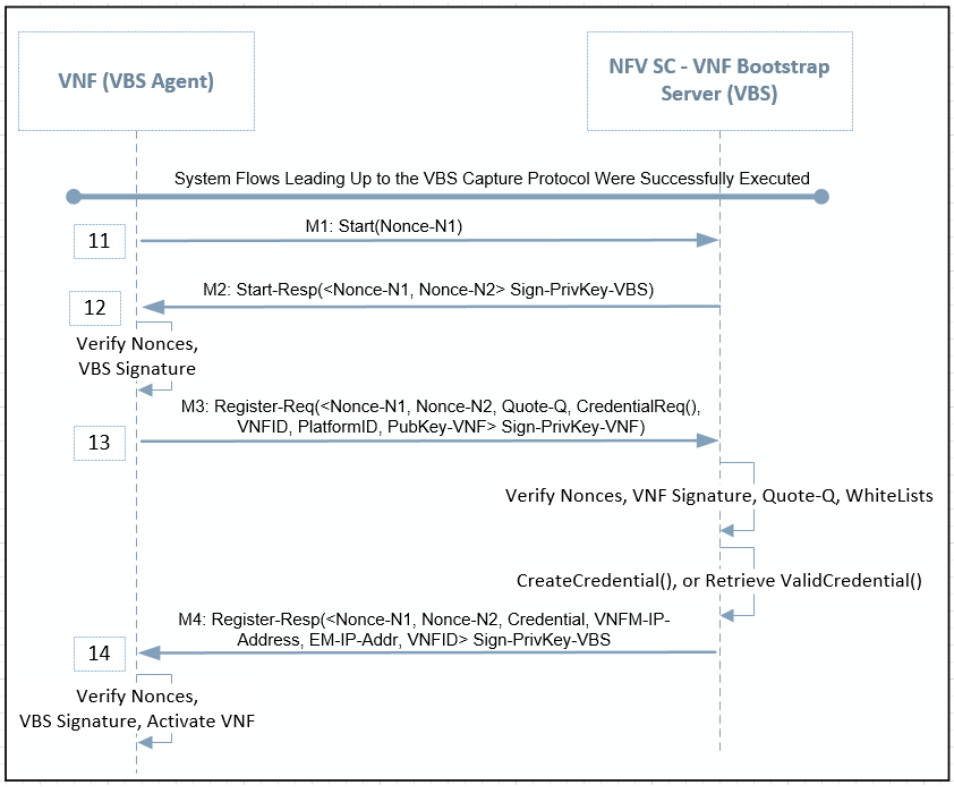

Figure 23: Secure Capture Protocol

The secure Capture protocol messages are described below.

Message M1: VBS Agent ➔ VBS: Start:

- The Start message that kicks off the Capture protocol with a uniquely generated fresh Nonce. A Nonce is a random number of adequate size.

Message M2: VBS ➔ VBS Agent: Start-Resp:

- Caches the session identified by Nonce-N1.
- Generates the Nonce-N2 and sends both Nonces back, with the message signed by the Private Key of the VBS.

Message M3: VBS Agent ➔ VBS: Register-Req:

- Verifies VBS Signature, Verifies the Nonce-N1.
- Caches the session of Nonce-N1 and Nonce-N2.
- Appends the Quote-Q, which is signed by the HMEE of the platform.
- Generates and sends the Credential Request, in addition to the VNF-ID, Platform-ID, and it's Public Key (PubKey-VNF).
- Signs the message with its Private Key (PrivKey-VNF).

Message M4: VBS ➔ VBS Agent: Register-Resp:

- Verifies VNF Signature, Verifies the Nonce-N1 and Nonce-N2 for session instance.
- Verifies Quote-Q with the Public Key of the Platform HMEE.
- Verify the VNF instance, VNFM, EM against whitelists.

- Creates the root security credential(s), or retrieves an appropriate root key credential(s) for this VNF. This credential can be a signed public key, a signed token or any other credential depending on the security infrastructure and policies.
- Generates and sends the Nonce-N1, Nonce-N2, Credential, VNFM IP address, EM IP address, and VNF-ID, message, signed by the Private Key of the VBS.

Message 4 Processing by VBS Agent:

- The VBS Agent verifies the message signature, Nonce-N1, Nonce-N2.
- The VBS Agent secures the received Credential.
- The VBS Agent is ready to activate the VNF.
- The VNF (including the Security Monitoring SSAs and VSFs) can use this security credential to securely connect with theit VNFM and EMs.

7.6.5 VNF Secure Personalization and Policy Protocol

Subsequent to the successful secure launch and instantiation of a VNF, and successful completion of the VNF Secure Bootstrapping protocol as defined in the previous clauses, the VNF is now activated. As discussed earlier, these VNF protocols are applicable to Security Monitoring SSAs, VSFs, VNFs, VNFCs, and application VMs. This VNF now needs to be personalized, which includes secure configuration with initial set of parameters, provisioned with appropriate meta data and state, establishing state for inter-VNF connections as in Service Function Chains, and seeded with any other VNF-specific information. Personlization also includes secure delivery of VNF vendor specific private information, including security credentials, as identified in [1].

VNF personalization is followed by a secure delivery of a startup set of policy and behavioural parameters for that VNF. These VNF policy and parameters are usually dynamic and dependent on deployment security policy and procedures. Policy can be delivered at initial post-secure bootstrap time and also during active execution of the VNF. Secure policy updates to VNFs are necessary to maintain consistent state across the entire system deployment, including NFV and traditional networks.

For NFV systems, the personalization and policy protocols are dynamic and automated. In an orchestration-driven system, VNFs will be dynamically and securely installed, and expected to follow the protocols defined in figure 24.

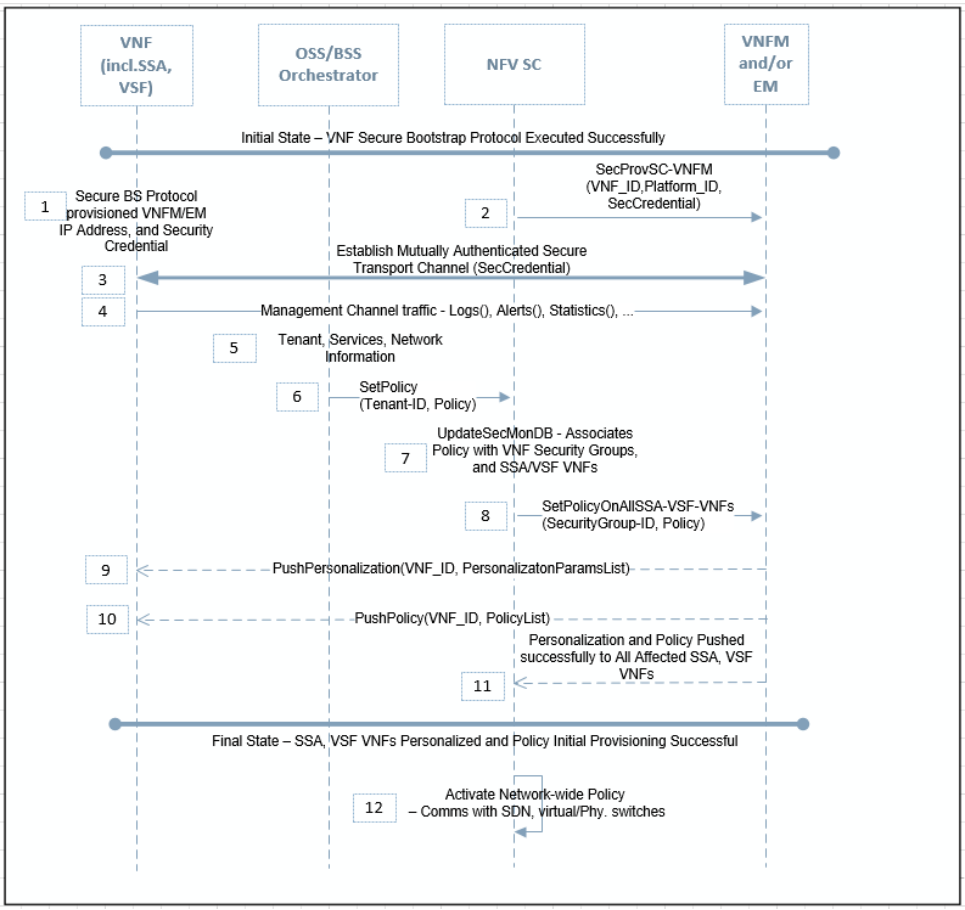

Figure 24: Secure VNF/SSA Personalization and Policy Protocol: Initial Provisioning

Personalization and Policy Protocol for Initial provisioning is described in this clause. A necessary prerequisite is the prior secure and mutually authenticated establishment of an encrypted, integrity and replay protected communication channels between the various management entities: OSS/BSS ⇔ NFV Orchestrator; NFV Orchestrator ⇔ NFV Security Controller; NFV Security Controller ⇔ VNFMs and EMs; NFV Security Controller ⇔ SecMonDB; And, the secure bootstrap protocol enables a secure channel between the dynamically instantiated VNFs and their VNFM and EMs:

1) At the successful execution of the Secure Bootstrap protocol, the VNF has been secure instantiated and provisioned with the IP address (or, any other reachability mechanism) of its VNFM and EM, and the initial root security credential(s) that uniquely identifies and would be used in a mutual authentication between this VNF and its VNFM/EM.

2) In a secure, Out of Band provisioning step, the NFV Security Controller will provision the VNFM and EM with the VNF_ID, Platform_ID, and the same Security Credential that the NFV Security Controller provisioned into the VNF. This step is a prerequisite for the secure and trusted established communication channel between the VNF and its VNFM.

3) The VNF and the VNFM/EM perform a mutually authenticated key exchange procedure using the security credentials, provisioned in the steps above. This choice of mutual authentication security protocol will be established by the security policy of the NFV deployment, and in most scenarios might be TLS.

4) Once the secure and trusted channel is setup, the VNF (incl. SSA, VSF) opens a management channel to its VNFM/EM. This channel is now used by the VNF to communicate management information (logs, alerts, statistics, etc.) with its VNFM/EM.

5) At the time a new tenant, network, service or capability is provisioned within the OSS/BSS or the Service Console, the OSS/BSS system communicates this new tenant, service, or network provisioning to the NFV Orchestrator.

6) The NFV Orchestrator is responsible for securely communicating the new tenant or service information to the NFV Security Controller. Security Controller will associate a set of Security Monitoring SSAs (VSFs) with the tenant, service or network. This is based on the security policy of this new tenant, service, or network designed by the NFV Security Controller. Policies are identified with Tenant ID, and associated with configurable security groups or other programmable structures or databases established in the NFV deployment. In most cases, a tenant domain administrator may also assign and deploy their appropriate Security Monitoring SSAs (incl. VSFs) to their workloads for NS-level security monitoring. It is expected that the NFV Orchestrator and the NFV Security Controller have a secure mutually authenticated channel. Establishing this secure channel is outside scope of this procedure.

7) The NFV Security Controller updates the SecMonDB with the new policy for the tenant, service or network, and the associated security group(s) or other security policy information. This allows long term retention and access of sensitive security policy information. The contents of this DB may optionally be encrypted, based on NFV deployment security policy. The policies will exist in the OSS/BSS system, as well. It is envisioned the OSS/BSS and NFV SC are broad systems and maintain their separate databases for policies including formats, storage encryption requirements, different access controls, etc. Over time, the OSS/BSS and NFV SC policies will merge into a unified DB.

8) The NFV Security Controller distributes the new security policy across to all VNFMs and EMs that are responsible for managing the Security Monitoring SSAs or VSFs. This policy distribution has to happen over a reliable protocol, with the NFV Security Controller maintaining state and ensuring policy consistency and delivery assurance across the entire network. In some tenant administrative domain cases, the Tenant's NFV Security Controller delivers policy to their VNFMs and EMs that manage their Physical Network Functions or Hybrid Network Functions.

9) The VNFM(s) and EMs push the VNF/VSF personalization data to all their VNFs/VSFs that are affected by the new tenant, service, and/or network provisioning. This personalization data distribution has to happen over a reliable protocol with the VNFMs/EMs maintaining state and ensuring that all VNFs/SSAs/VSFs have received the personalization data. Personalization data includes secure configuration data, initial set of VNF parameters, meta-data, connection information about other VNFs, vendor-specific information, performance, traffic engineering, and QoS parameters and policies, etc. These are the data and components that the newly instantiated VNF needs to get ready for processing workload traffic.

10) The VNFM(s) or EMs push the tenant, service, and/or network policy to all their SSAs (incl. VSFs). This policy distribution has to happen over a reliable protocol with the VNFMs maintaining state and ensuring that all VNFs/VSFs have received the policy data. The policy list includes tenant specific security processing policy, security traffic policy, security groups, network services processing policy, etc.

11) On successful completion of all Personalization and Policy updates, the VNFM(s)/EM(s) report back to the NFV Security Controller. The VNFM(s)/EMs will also report back all failures and errors that might have occurred. The NFV Security Controller will process all responses and issue alerts and status updates to the Security administrator, including securely logging.

12) On receiving all successful responses, the NFV Security Controller will activate network wide security policy for the traffic. To enable and activate traffic for the tenant, the NFV Security Controller will securely communicate with network-wide traffic switching elements, including SDN Controllers, Openstack Neutron Plugins, various virtual and physical Switch/Router Managers, etc.

Security Monitoring SSAs, including VNFs, VSFs and SSAs in the NFVI hypervisors and physical devices will follow the VNF Secure Bootstrap protocol and VNF Personalization and Policy protocols as described here-in. In addition, these protocols will be followed by other Tenant VNFs like NS, SFCs and application VMs.

In normal NFV operation, Security Monitoring VNFs/VSFs will be instantiated and triggered with personalization and policy information as per protocols defined above. In a dynamic and automated NFV deployment, it is expected that existing services, tenants, networks policies will be updated and would have to be securely and consistently pushed across the NFV deployment, including to any physical/hybrid network functions, as dictated by the security policy.

This security and monitoring update can occur in many scenarios, including addition or removal of tenants, tenant workload migration, update tenant's SLA and QoS, Geo-based or regulatory requirements updates, failures or HA configurations of current Monitoring VNFs/VSFs, etc. Security policy updates are also expected as a remediation action of the automated security response within an NFV deployment, especially for security threat mitigation, malware response, network DoS attacks, and other such threat remediation scenarios.

The NFV Security Controller is expected to orchestrate the new Security policy across the NFVI administrative domain, and within each tenant's virtualised and physical deployments. Security Monitoring policies are part of administrative domain of NFVI hence are orchestrated from the NFV SC. Tenants also have their security monitoring policies that can be orchestrated by the Tenant's Security Controllers to their SSAs.

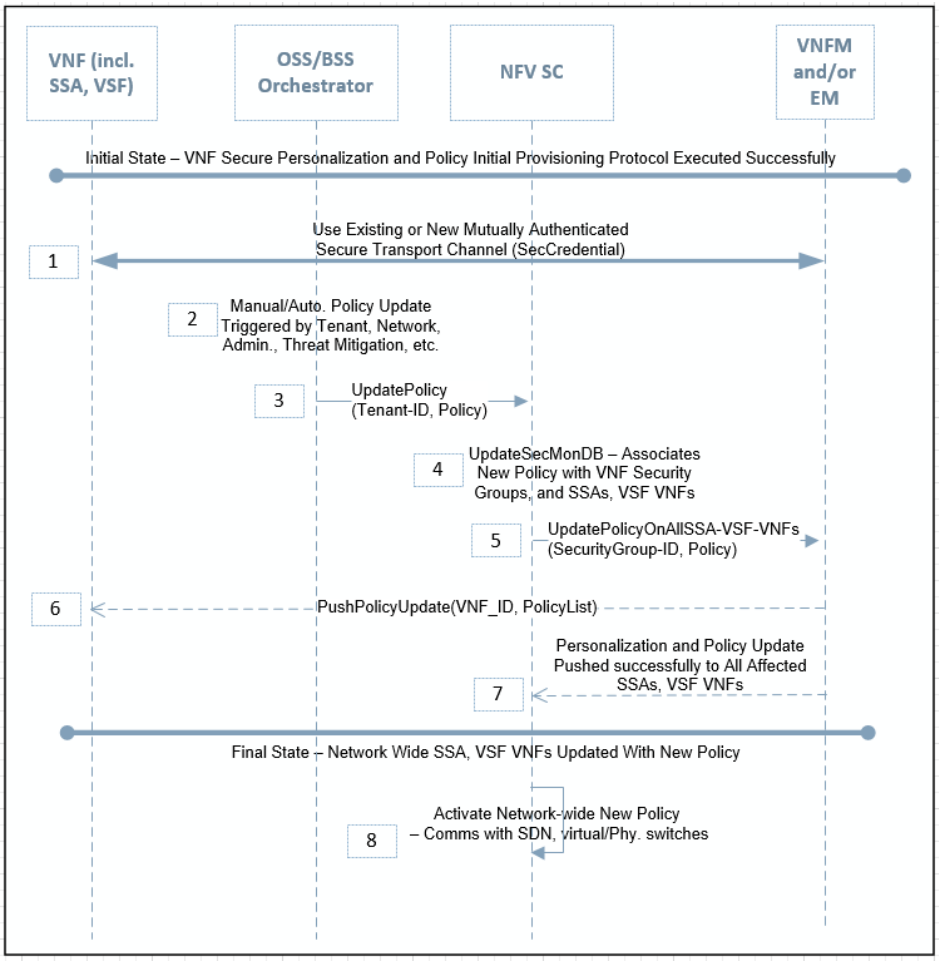

Figure 25: Secure VNF Personalization and Policy Protocol: Provisioning Update

Update procedures for Personalization and Policy Protocol are described below. It is expected that the Provisioning and Policy Protocol - Initial Provisioning, as described above, has successfully been executed:

1) The Monitoring SSAs, VSFs and the VNFM/EM have a secure, mutually authenticated channel, as described in earlier flows. The same channel may be used, or as per NFV security deployment policy, a new secure channel may be set up for this procedure to ensure security credentials are still current and active.

2) A system event may trigger the Secure VNF Personalization and Policy update procedure. As described above this trigger may be add/remove tenants, response to a network or system threat, site security policy updates, etc. These system events may be automated, manual, time-driven, and/or dynamic.

3) The new security policy is added by the NFV Security Controller triggered by events from the OSS/BSS and Orchestrator, and security monitoring analytics system.

4) The NFV Security Controller will update the new security policies, security groups, and other associated configurations into the SecMonDB. Update of this secure database will follow the same security procedures as were used for Initial Provisioning steps of this protocol.

5) The NFV Security Controller will send a secure Policy update to all affected VNFMs/EMs. The Security Controller tracks the VNFMs/EMs for all Security Monitoring SSAs, VNFs/VSFs in the deployments.

6) The VNFM(s) and EM(s) will push new policy updates to all affected SSAs, VNFs/VSFs. This update will follow the same secure and reliable delivery that used in the Initial Provisioning steps of this protocol. It is important that the SSAs/VNFs/VSFs behaviour follow the prescribed security enforcement procedure. This means that based on the pre-set security policy or the update priority or flags, a SSA/VNF/VSF may immediately abandon its execution, gracefully exit, block all traffic, continue execution until another trigger, etc.

7) The VNFM(s) and EM(s) will report success back to the NFV Security Controller, similar to the Initial Provisioning steps of this protocol. At this point, the new security policies have been pushed into the entire network (incl. NFV, Physical and/or hybrid networks).

8) Based on security policy of NFV deployment, the new policies are now activated by the NFV Security Controller. This follows same procedure as specified in the initial provisioning steps of this protocol.

Successful execution of this update protocol should ensure a secure, consistent new state of the NFV deployment, including mixed deployments with physical security functions.

7.7 NFV Deployments

7.7.1 Deployment Scenarios

This clause discusses various mechanisms which could be used for Security Monitoring in an NFV deployment. It would be based on the mechanisms by which a VNF/VNFC interacts with other VNF/VNFCs.

7.7.2 vTAP Deployment Model

There can be different forms of virtual tap (vTap) and virtual Front-End Processor(s) (vFEP) based on the NFV deployments in the network. These could serve as selective-filtering or splicer role, and in some case, might also be part of the service chain. This will then be fully-aware of the NFV Service orchestrator such that when VNFs move, grow/suspend due to scale-out/scale-in, vTap will be always in place.

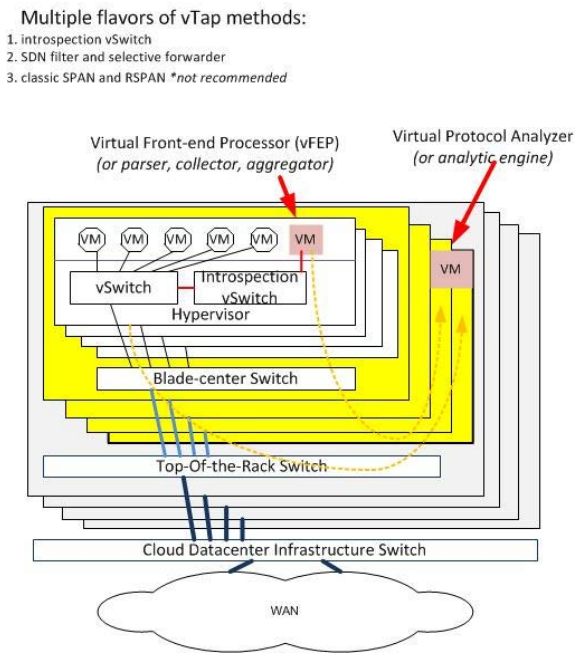

Figure 26: Sample Virtual TAP Deployment Scenario

Figure 26 illustrates a sample of vTAP deployment in a virtualised network environment that are based on NFV placement. The vTAP deployment may also be in the virtual or physical NIC or Switch.

vFEP is a pre-processor intended to perform some basic filtering rules (called pre-filter) to be applied to deliver telemetry to the Security Monitoring Analytics System. The prefilter ruleset is highly tuned to the specific VNF workload of interest and has to be refined on as needed basis.

The vTAP is used to tap specific "VM of interest" (e.g. VMs running a specific NFV function, or on NIC or Switch). Based on specific workload type and the job the VM host is configured, one or few vNIC will be the point of interest. Based on the specific workload type, may be a specific traffic pattern (as defined by e.g. 5 tuples) will be filtered by vTap. Since the VNF workload(s) can move, grow or shrink, such tapping arrangement has to have a close tie with NVF Orchestration system and needs to be constantly in-sync with the current VNF state/topology. The introspection vSwitch (i.e. vTap) follows the known VNF state/topology and perform the necessary tapping and filtering to only capture the traffic of interest. Each physical host has a light weight VM that performs the vFEP (virtual front end processing) to filter/refine/reduce the data set, from the in-scope local VMs that run the current VNF workloads. In order to make the vSwitch interoperable, it is suggested to make the V-Switch compatible with OpenStack supported Neutron.

NOTE: vFEP is always resident in all hosts that are in-scope for VNF production platform:

- Individual vFEP forms the tributary to deliver the condensed/pre-processed captured traffic to the centralized Analytic System.

Centralized Analytic System has the end-to-end view of various tapping points and can consolidate and correlate traffic to derive a top-down view of the overall VNF system to achieve part of the security monitoring mandate of VNF.

7.7.3 VNF Integrated Security Monitoring

In this deployment, Security Monitoring and DPI functions may potentially be integrated as part of VNFs such as MME, HSS in signalling plane or PGW and SGW in data plane. In those scenarios it will possibly, reduce the need for additional vProbes in the virtualised environment.

While integrating DPI functionality as part of VNF provides additional advantage since it reduces the complexity of maintaining additional virtual probes, and many of the correlation between data and signalling can be done within an VNF, this deployment scenario may affect the performance of the VNFs as the DPI is very much CPU intensive. It also needs additional considerations for integrating with threat management system including supporting APIs. It is suggested to conduct a study to investigate the pros and cons of integrated DPI as part of VNFs (e.g. PGW, MME). There needs to be a study regarding the effect of integrated DPI and different modes of deployment and how both performance and scalability can be obtained by proper load balancing.

Annex A (informative): Authors & contributors

The following people have contributed to the present document:

Rapporteurs:

- Mr Ashutosh Dutta, AT&T
- Mr. Kapil Sood, Intel Corp.
- Ms. Wei Lu, Nokia

Other contributors:

- Mr. Michael Bilca, OTD
- Mr. Mike Bursell, Redhat
- Mr. Scott Cadzow, Cadzow Communications
- Mr. Igor Faynberg, Alcatel-Lucent
- Mr. Michael Lazar, DataArt
- Ms. Hui-Lan Lu, Alcatel-Lucent
- Mr. Alex Leadbeater, BT
- Mr. Manuel Nedbal, Intel
- Mr. Stephane Mahieu, Nokia
- Ms. Jing Ping, Nokia
- Mr. Anand Prasad, NEC
- Mr. Pradheep Kumar S., NEC
- Mr. Esa Salahuddin, Cisco
- Mr. Mihai Serb, Huawei
- Mr. Ching Shih, ATT
- Mr. Gurpreet Singh, Spirent
- Mr. Prabhu T., NEC
- Ms. Anne-Marie Praden, Gemalto
- Mr. Marcus Wong, Huawei

History

Document history		
V3.1.1	February 2017	Publication