FÉDÉRATION FRANÇAISE DES TÉLÉCOMS

Référentiel d'objectifs de sécurité en matière de fonctions réseau virtualisées

Table des matières

Liste des figures

Liste des tableaux

1 Préambule

Ce document de travail constitue le 'Référentiel d'objectifs de sécurité en matière de fonctions réseau virtualisées', réalisé par Internet of Trust pour le compte de FFTélécoms.

- Donneur d'ordre : FFTélécoms
- Entretiens et validation des livrables : Bouygues, Orange et SFR
- Coordinateur et éditeur des documents : Internet of Trust

Le comité de pilotage était composé de représentants de Bouygues (Mr Jean-Pierre BAREIT), Orange (Mr Jean-Philippe WARY), SFR (Mr Julien ESPOSITO) et FFTélécoms (Mr Alexandre GALDIN).

Ce document a été réalisé par un groupe de travail constitué des personnes suivantes

• Mr Alexandre GALDIN	FFTélécoms
• Mr Stive ANDJANGA	Bouygues Telecom
• Mr Jean-Pierre BAREIT	Bouygues Telecom
• Mr Cyril DELÉTRÉ	Orange
• Mr Jean-Philippe WARY	Orange
• Mr Julien ESPOSITO	SFR
• Mr Eric MATTERA	SFR
• Mr Jean-Baptiste FOUAD	SFR
• Mr Mohamad HAJJ	Internet of Trust
• Mme Claire LOISEAUX	Internet of Trust

2 Synthèse

La FFTélécoms souhaite disposer d'un référentiel d'objectifs de sécurité à atteindre pour les OCEs (Opérateurs de communications électroniques) en matière d'équipements et infrastructures virtualisées et les futures applications de 5G. Ce référentiel est destiné à fournir une protection des applications (principalement en préservant l'isolation) s'exécutant sur des infrastructures virtualisées. Il identifie les obligations et contraintes de sécurité à respecter par les OCEs/Fournisseurs et définit les objectifs de sécurité avec les contremesures associées.

Ce document est un référentiel qui vise à être une base de référence afin de permettre aux OCEs d'effectuer une partie des analyses et des tests de sécurité demandées par l'ANSSI. Ces analyses et tests de sécurité sont indispensables avant tout déploiement de services sensibles. Le rapport rédigé à l'issue des analyses et tests de sécurité est transmis à l'ANSSI.

Ce référentiel est focalisé sur les objectifs de sécurité à mettre en œuvre qui sont liées à la virtualisation et à la mutualisation des fonctions réseaux (périmètre). Dans le cadre d'un audit il vient compléter les référentiels existants concernant les aspects hors périmètre (voir section 4.4).

Ce document concerne :

- Les OCEs qui peuvent utiliser ce référentiel pour construire leur analyse de sécurité.
- Les équipementiers (fournisseurs des matériels et éditeurs de logiciels) qui doivent fournir des solutions permettant d'atteindre les objectifs fixés dans le référentiel.
- Les auditeurs (internes ou externes) qui peuvent utiliser ce référentiel et l'analyse de sécurité associée comme base de leur plan d'audit.
- L'ANSSI qui pourra s'appuyer sur le respect des objectifs de ce référentiel par les OCEs lors de ses propres analyses de sécurité.

Les objectifs de sécurité concernent essentiellement l'isolation des différentes fonctions réseaux (VNF) lorsque les ressources (Nœud de calcul, espace de stockage, etc.) sont mutualisées. Les objectifs de sécurité mentionnés dans ce document visent à diminuer autant que possible la surface d'attaque des infrastructures mutualisées lors des déploiements.

Plusieurs scenarios de mutualisation ont été imaginés pour :

- Répondre aux souhaits des OCEs.
- Prendre en compte le niveau de sécurité disponible dans les équipements des fournisseurs.
- Prendre en compte le niveau de sensibilité des VNFs.
- Prendre en compte les méthodes liées à l'exploitation des dispositifs ainsi que le cloisonnement des rôles.
- La disponibilité de la solution.

- La journalisation des événements et notamment ceux liés à la sécurité.

Note : Dans la suite de ce document, on utilise la notion 'sensibilité' des VNFs en tant que critère de mutualisation.

Le degré de sensibilité des VNFs sera issu d'une analyse de risques qui prend en compte différents critères dont l'exposition et la sensibilité des données manipulées.

A l'issue de l'analyse de risque, les OCE mutualisent les VNF en fonction de leur niveau de sensibilité et degré d'exposition (voir la section 'Définitions' pour des exemples sur la classification des VNFs).

L'analyse de risques n'est pas faite dans ce document. Elle pourra faire l'objet d'un document complémentaire FFT ou spécifique pour chaque opérateur.

Note : Les notions 'qualification' 'certification' et 'autorisation' figurant dans le document sont portées actuellement par l'ANSSI suivant les règlementations nationales en France. L'ANSSI est l'autorité ayant le pouvoir de délivrer des autorisations, des qualifications et des certifications et de s'appuyer sur des auditeurs PASSI.

Il est prévu de transposer ces dispositions dans un cadre européen (par exemple selon un schéma européen conforme au CyberAct) lorsqu'il sera disponible et engagé.

Note : Ce document n'est pas une analyse de risque. Ce sont des exigences sous forme de profil de protection.

3 Introduction

3.1 Objectif

Les objectifs de sécurité décrits dans ce document doivent être :

- Sélectionnés en fonction de la cible technique spécifique que l'OCE souhaite réaliser ;
- Pouvoir être couverts par les OCEs et les équipementiers ;
- Pouvoir être vérifiés en interne et/ou par un tiers ;
- Validés par l'ANSSI ou dans un cadre européen lorsq'il sera disponible.

3.2 Choix du périmètre

Il a été décidé de concentrer l'étude sur le socle au sein du cœur de réseau qui est composé de l'Infrastructure de virtualisation (NFVI) et les fonctions réseaux VNF.

Les fonctions suivantes sont dans le périmètre de l'étude :

- Optimisation des ressources SW et HW avec la co-localisation et la virtualisation ;
- Mutualisation des VNF ;
- La sécurisation du socle ;
- Approvisionnement multifournisseur.

3.3 Structure du référentiel

Le référentiel est organisé de la façon suivante :

- Le périmètre de l'étude et l'architecture du socle ;
- Les aspects identifiés restant à traiter ;
- La liste des prérequis pour les équipements, utilisateurs et l'environnement physique ;
- Les données sensibles à protéger ;
- Les utilisateurs du socle ;
- Les menaces ;
- Les objectifs de sécurité à atteindre et
- Des exemples de contremesures de sécurité visant à protéger les données sensibles, à limiter l'impact des menaces et à répondre aux objectifs de sécurité.

3.4 Inputs

Le document est construit en se basant sur les informations collectées pendant les entretiens avec les OCEs ainsi que les documents suivants :

1. ETSI GS NFV 002: Network Functions Virtualisation (NFV) – Architectural Framework.

2. ETSI GS NFV-SWA 001: Network Functions Virtualisation (NFV) – Virtual Network Function Architecture.
3. ANSSI – Note technique 3659/ANSSI/SDE/DR : Principes de sécurisation applicables aux plateformes virtuelles supportant des fonctions de télécommunications.
4. 5G PPP 5G Architecture White Paper Revision 2.0 – (White Paper version 2.0 December 2017).
5. 5G PPP Security Landscape – (White Paper) June 2017.
6. 5G-PPP Vision on Software Networks – (White Paper) January 2017.
7. 5G PPP 5G Architecture – (White Paper) Updated July 2016.

3.5 Références internes

Les références internes sont les suivantes :

1. Définition du cadre et présentation faite lors de la réunion avec l'ANSSI.
2. Les comptes rendus des entretiens avec les OCEs.

3.6 Glossaire

3.6.1 Acronymes

AF	Application Function
AMF	Access and Mobility Management Function
AUSF	Authentication Server Function
CDMA	Code division multiple access
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile Communications
HSM	Hardware Security Module
IMS	IP Multimedia Core Network Subsystem
LTE	Long Term Evolution
N-CA	Nœud de calcul pour les VNF
N-CO	Nœud de contrôle pour le VIM
MANO	Management and Orchestration
NEF	Network Exposure Function
NFV	Network Functions Virtualization (ETSI)
NFVI	Network Functions Virtualization Infrastructure (ETSI)
NRF	Network Repository Function
OCE	Opérateurs de communications électroniques
PCF	Policy Control Function
RAN	Radio Access Network
SIEM	Security information and event management
SMF	Session Management Function
TPM	Trusted Platform Module
UDM	Unified Data Management
UPF	User Plane Function
VIM	Virtualised Infrastructure Manager

VL	Virtualisation Layer
VM	Virtual Machine
VNF	Virtual Network Function
VNFM	Virtual Network Function Manager
WCDMA	Wideband Code Division Multiple Access
Wifi	Wireless Fidelity

3.6.2 Définitions

- Cœur de réseau : est constitué de plusieurs fonctions réseaux, dont certaines virtualisées (les VNF).
- Équipementiers : sont les différents fournisseurs des VNF, nœuds de calcul, nœuds de contrôle, équipements réseau, équipements de stockage, etc. (eg Nokia, CISCO, HP, Ericsson).
- Hyperviseur : composant logiciel qui joue le rôle d'interface entre les machines virtuelles et l'infrastructure physique. Des exemples des logiciels pouvant être mis en œuvre pour jouer le rôle d'un hyperviseur sont entre autres KVM OpenStack, VMware ESXI, Hyper-V, etc.
- HSM : Module matériel de sécurité qui offre des fonctions cryptographiques consistant à générer, stocker et protéger des clés cryptographiques.
- NFVI : infrastructure virtualisée du socle, c'est à dire le socle sans les VNF.
- Nœud de calcul : serveur dédiée à l'hébergement et l'exécution des VM constituant une ou plusieurs VNF.
- Nœud de contrôle : serveur dédié à l'exécution du VIM.
- Orchestrateur (NFV Orchestrator) : L'entité d'orchestration est responsable du cycle de vie des services réseau tant au niveau logiciel que matériel sur plusieurs domaines en contrôlant les VIM de chaque domaine.
- Plateforme de réseau : Ce composant assure la communication entre les socles.
- PMR : Les réseaux mobiles professionnels (souvent rassemblés sous le sigle PMR pour " Professional mobile radio ") sont des réseaux mobiles indépendants d'ampleur généralement locale ou régionale, exploités pour des usages professionnels.
- Socle : Infrastructure (NFVI) regroupant des ressources matérielles (nœuds de calcul et de contrôle, switch, stockage commun, …) et logicielles (hyperviseur, …) qui peuvent être mutualisées entre plusieurs VNF.
- Stockage Commun : mémoire de masse partagée par les nœuds de calcul du même site.
- TPM : Module de plateforme sécurisée qui fournit une protection des clés utilisées pour assurer le démarrage sécurisé de l'hyperviseur.

- VNF réseau : fonctions réseaux déployées par OCE en tant qu'instances virtualisées au lieu d'entités matérielles dédiées. Ces services VNF incluent le routage, les fonctions pare-feu, l'équilibrage de charge, etc.
- Niveau de sensibilité des VNF : La sensibilité d'une VNF est déterminée par une analyse de risque[1]. Le niveau de sensibilité dépendra principalement de sensibilité des informations manipulées. Cette sensibilité doit être évaluée en fonction :
    - De la nature des informations sensibles détenues par les machines virtuelles ;
    - De la nature des fonctions de télécommunication virtualisées ;

  Dans le cadre de ce référentiel on définit deux niveaux de sensibilité :
    1. Sensibilité critique qui porte sur
        - Les VNFs embarquant des fonctions IL
        - Les VNFs tierces sensibles (par exemple exécutant des services pour des OIVs)
        - Les VNFs sensibles pur OCE (par exemple les VNFs ayant en charge les fonctions d'administration et d'exploitation ainsi que les fonctions d'authentification).

      Cette notion pourra être étendue selon les usages futurs du réseau 5G.
    2. Sensibilité non critique pour les VNFs non listées ci-dessus.
- VNF tierce : VNF d'un fournisseur de service tiers qui peut être plus ou moins sensible en termes de bande passante et/ou de sensibilité des informations manipulées. Exemples : énergie, voiture autonome, chirurgie à distance (CF verticaux listés dans la GSMA).
- Données sensibles : données à protéger en confidentialité et intégrité (à titre d'exemple les interceptions, les clés IL, les clés VNFs et hyperviseur, les fichiers de description des VNFs, mots de passe, journaux, les données personnelles, informations bancaires, etc.).
- Fonctions sensibles au sein du socle, à titre d'exemple :
    - L'ajout de comptes, changement des clés d'authentification des comptes d'administration,
    - La configuration des VNFs et de l'hyperviseur
    - Les fonctions IL
    - L'administration réseau
    - Les ajout/suppression/Update des VNF
    - La mise à jour du Firmware/SW/HW

[1] L'ANSSI et les OCEs pourraient travailler ensemble à la définition d'une typologie générique des VNF les plus courantes suivi d'une typologie spécifique au cas par cas selon le fournisseur et l'implémentation des VNFs. Cette typologie permettra de déterminer à quelles conditions les VNF choisies peuvent s'exécuter sur une même NFVI.

- La gestion des droits d'accès
- La gestion des clés cryptographiques
- La configuration des VIM, VNFM, et VNF
- La configuration des nœuds de calcul et contrôle, Switch, routeur, stockage,
- etc.

- Exposition :
  - Le degré d'exposition des VNFs est déterminé par une analyse de risque. Il signifie qu'elles sont exposées ou non aux mêmes chemins d'attaques et/ou aux mêmes possibilités d'accéder / de commander les VNFs à distance. Le degré d'exposition des VNFs est une donnée déterminante pour la classification de niveau de sensibilité des VNFs.
  - L'exposition concerne l'accès aux VNF à travers de manière non limitative : des applications tierces, à des fournisseurs ou administrateurs différents, à d'autres VNFs, à internet, à des réseaux privés, etc.
  - On définit trois degrés d'exposition :
    - Une VNF qui expose directement une ou plusieurs de ses interfaces vers l'extérieur du réseau de production devra avoir un degré d'exposition élevé. On parle de l'exposition à des zones de confiance différentes (notamment les accès au réseau public, ou à un réseau privé, ou à du trafic des abonnés, ou à des interfaces externes vers d'autres OCEs, etc.) ;
    - Les VNF ayant une ou plusieurs interfaces directement reliées au système d'information ou au réseau bureautique devront avoir un degré d'exposition moins critique ;
    - Un niveau d'exposition faible à des mêmes zones de confiance.
    - Les VNF n'ayant d'interface qu'avec des zones de confiance de niveau identique.

4 Description du périmètre

Le périmètre de l'étude est le socle du cœur de réseau composé de l'infrastructure virtualisée (NFVI) avec les fonctions de télécommunications (VNF) contribuant à l'acheminement des communications.

Ce chapitre décrit le périmètre de l'étude, les propriétés étudiées, l'architecture globale, les utilisations et les fonctions de chaque composant de l'infrastructure virtualisée.

En fin de chapitre, nous identifions les limites du périmètre avec une description succincte des éléments identifiés dans le cadre de l'étude qui ont une contribution à la sécurité du socle mais qui n'ont pas été considérés faute de temps et de ressources.

4.1 Périmètre de l'étude concernant les propriétés étudiées

Les propriétés principales étudiées dans le cadre de cette étude sont entre autres les suivantes :

1. **Isolation** des VNF au sein du socle :
    a. Isolation de VNF de même sensibilité.
    b. Isolation de VNF de sensibilités différentes.
    c. Isolation entre VNF et les nœuds de calcul
    d. Isolation entre VNF et l'hyperviseur
    e. Isolation entre VNF et l'orchestrateur
    f. Isolation entre VNF et la plateforme de routage
2. **Traçabilité** des opérations et des actions sur toutes les interfaces internes et externes du socle.
3. **Gestion des identités et des accès** : Authentification des utilisateurs et les mécanismes mis en œuvre pour garantir la confidentialité et l'intégrité des crédentials, l'imputabilité et la traçabilité des accès.
4. **Gestion des secrets cryptographiques** :
    a. Les fonctionnalités de chiffrement, aussi bien au niveau des flux de données qu'au niveau des données au repos.
    b. Les solutions technologiques assurant une gestion sécurisée des clés cryptographiques (par exemple l'utilisation d'un HSM qualifié).
    c. Les solutions technologiques assurant un démarrage sécurisé de l'hyperviseur (exemple : utilisation d'un TPM).
5. **Journalisation** des évènements et centralisation des journaux.
6. **Administration** : Cloisonnement des fonctions d'administration.
7. **Mise à jour et déploiement** des correctifs.
8. **Localisation et protection** des données personnelles (conformité au RGPD).
9. **Disponibilité** des équipements matériels et logiciels du socle.

Ces propriétés sont étudiées dans le cadre de la mutualisation des ressources de l'infrastructure virtualisée NFVI pour l'hébergement de plusieurs VNF.

La mutualisation peut intervenir au niveau de différents composants du socle :

1. Mutualisation des VNF : plusieurs VNF s'exécutent sur le même socle.

2. Mutualisation du VNFM : un VNFM unique pour piloter plusieurs VNF différentes.
3. Mutualisation du VIM : un VIM unique afin de contrôler des nœuds de calcul (serveur physique) exécutant des VNF différentes.
4. Mutualisation des ressources physiques :
    a. Équipements réseau : Utilisation des mêmes équipements réseau afin de connecter l'ensemble des nœuds de calcul.
    b. Équipements de stockage : Utilisation des mêmes équipements de stockage afin d'héberger toutes les données et les images des différentes VNF.
    c. Nœuds de calcul : Exécution des VNF différentes sur un même nœud de calcul.

4.2 Périmètre de l'étude concernant l'architecture

Le périmètre dans le cadre de cette étude couvre l'infrastructure virtualisée sur une base NFV, applicable en particulier à la virtualisation des fonctions réseau VNF au sein du cœur de réseau.

Le périmètre couvre le socle avec les VNF réseaux. Les VNF tierces (Automobile, Santé, …) et les réseaux mobiles professionnels (PMR) ne font pas partie du périmètre de l'étude. Celles-ci peuvent être présentées en bordure (voir Figure 2).

Le schéma fonctionnel du socle est illustré ci-dessous (Figure 1).

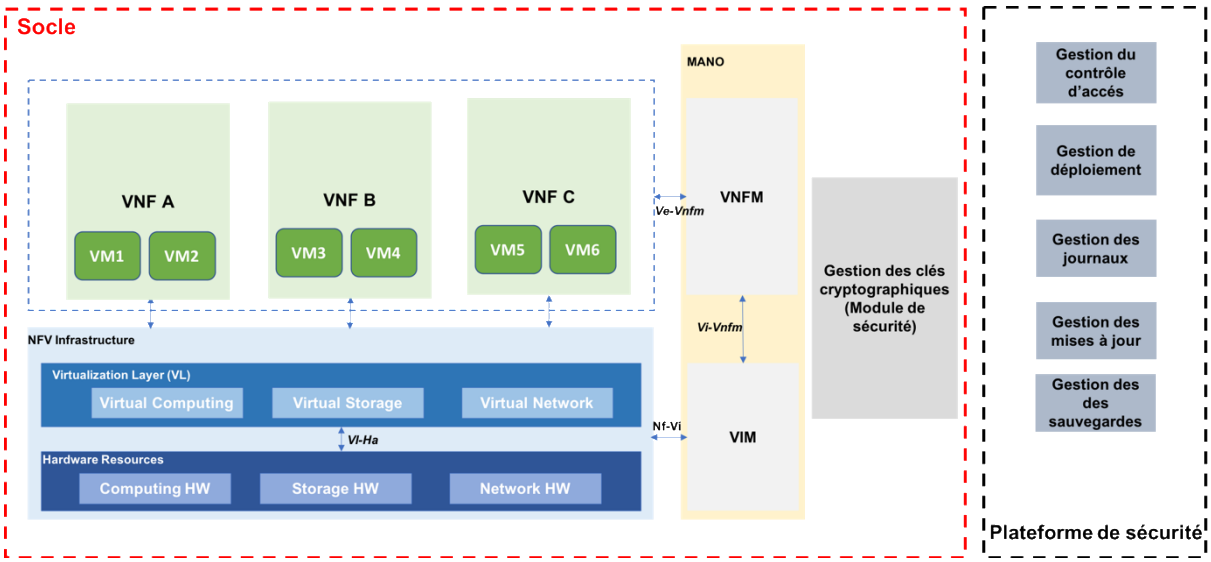

Figure 1: Architecture du socle

Le socle est constitué des composants suivants :

- L'infrastructure du NFV (NFVI) :
    - Équipements réseau matériels qui constituent l'infrastructure (commutateurs, routeurs, etc.).
    - Les nœuds de calcul (serveurs physiques) exécutant les VNF. Chaque nœud possède des ressources physiques : CPU, RAM, carte réseau et espace disque local. Il est possible que les VNF ne soient pas stockées sur l'espace disque du

nœud de calcul mais sur le stockage commun (centralisé pour plusieurs nœuds de calcul). Ainsi, chaque nœud de calcul peut exécuter n'importe quelle VNF.

  - Les nœuds de contrôle exécutant les VIM
  - L'hyperviseur exécutant les VM et les services de gestion de la virtualisation. Il est piloté par le VIM.
- Les fonctions réseaux virtualisées (VNF) pilotées par le VNFM.
- La gestion et l'orchestration (MANO)
  - Un VIM pour piloter et gérer les instances des hyperviseurs.
  - Un VNFM pour piloter et gérer les instances des VNF.
- Les différents types de stockage
  - Le stockage commun (e.g. images des hyperviseurs et des VNF et données des VNF en particulier lorsque l'espace local du nœud de calcul n'est pas utilisé) entre plusieurs nœuds de calcul du même site.
  - Une zone mémoire locale dans chaque nœud de calcul.

La plateforme de sécurité est dans le scope de l'étude mais ne fait pas partie du socle. Elle est composée des fonctions suivantes :

- Gestion du contrôle d'accès,
- Gestion des déploiements,
- Gestion des mises à jour. Elle doit s'envisager à plusieurs niveaux (infrastructure, composants de virtualisation, machines virtuelles etc.).
- Gestion des journaux.
- Gestions des outils.
- Gestion des sauvegardes.
- Gestion des événements de sécurité.

4.2.1 Infrastructure NFVI

L'infrastructure NFVI est une infrastructure virtualisée qui s'appuie sur une architecture physique pour fournir des fonctions de stockage, de calcul et de réseau. Il fournit les ressources matérielles et le logiciel de virtualisation.

Le NFVI se compose donc :

- De composants matériels (nœuds de calcul, switch, routeur, stockage commun, etc.) ;
- D'une interface virtuelle (stockage, réseau, calcul) ;
- D'une couche de virtualisation entre le matériel et le logiciel (Hyperviseur).

La couche de virtualisation (Hyperviseur) permet de découpler l'implémentation logicielle des fonctions réseaux (VNF) des ressources matérielles. L'hyperviseur est un logiciel critique du point de vue de la sécurité car il doit assurer l'isolation des ressources et de l'exécution. Il permet d'allouer les ressources matérielles distinctes aux différentes machines virtuelles (VM). Le partage de ressources obéit à des règles configurables précises (temps CPU, mémoire vive, priorités réseau, entrées sorties disque, etc.).

4.2.2 Les fonctions réseaux virtualisées (VNF)

Une fonction réseau (e.g. 5G VNFs : AMF, SMF, NRF, UDM, etc.) est formée d'un ensemble de VNF (hébergées/exécutées) sur NFVI. Les VNF sont déployées dans des instances virtualisées de type VM, Unikernels ou Containers suivant le niveau de performance ou d'isolation recherché. Une VM est une instance complète de système d'exploitation, avec son système de fichiers, ses comptes utilisateurs, ses processus, etc. Ainsi, les VM s'exécutant sur les nœuds de calcul sont considérées comme des applications pour ceux-ci. Sur un nœud de calcul, il est possible d'exécuter une ou plusieurs VM constituant une ou plusieurs VNF.

La couche de virtualisation fournie par la NFVI permet de s'affranchir des ressources matérielles pour raisonner uniquement au niveau des ressources logiques.

Néanmoins, pour continuer à assurer l'isolation des solutions des équipementiers (matériel, hyperviseur, VNF, VIM, …) entre eux et l'isolation des VNF de sensibilités différentes, les contre-mesures concernent aussi les niveaux HW et SW.

4.2.3 La gestion et l'orchestration (MANO)

La gestion et l'orchestration des VM est sous la responsabilité de la fonction MANO (Management and orchestration). La fonction MANO doit gérer les ressources de l'infrastructure NFVI (capacité réseau, la puissance de calcul, l'espace mémoire) et la durée de vie des fonctions virtuelles en fonctionnement sur l'infrastructure NFVI (création et allocation des VM). Il permet de gérer les services réseaux de bout en bout.

La gestion et l'orchestration NFV (MANO) automatise le déploiement de fonctions réseaux virtualisées (VNF) pour provisionner, configurer et tester les performances de ses fonctions. Pour cela, il faut superviser :

- L'infrastructure pour la gestion du matériel (capacité, réseau, calcul, …) ;
- Le déploiement de fonctions réseaux (VNF) ;
- Le chaînage de fonctions réseaux pour réaliser des services réseaux.

Le MANO est composé des blocs suivants.

4.2.3.1 VIM

Le gestionnaire (VIM) est en charge de la gestion des ressources du NFVI. Il est constitué des fonctions suivantes :

- Initialiser et paramétrer l'hyperviseur ;

- Définir les instances des VNF à mettre en œuvre et les besoins en ressources de chaque instance (CPU, mémoire, interface et réseau) ;
- Créer une VM à partir d'une image disque présente dans le catalogue du VIM ;
- Démarrer, arrêter, redémarrer une VM ;
- Supprimer une VM et ses données ;
- Accéder à la console d'une VM ;
- Consulter l'état de l'hyperviseur.

Le VIM est un composant logiciel qui s'exécute sur un ou plusieurs nœuds de calcul. L'infrastructure NFVI peut être gérée par plusieurs VIM. L'isolation entre VNF au sein de l'infrastructure virtualisée (NFVI) est assurée par la combinaison hyperviseur + VIM + composants hardware.

4.2.3.2 VNFM

Le gestionnaire (VNFM) est en charge du cycle de vie des VNF en fonction des données contenues dans le descripteur. Il charge l'image des VNF depuis le stockage commun, les démarre, les adapte, les met au rebut et il collecte les indicateurs de supervision. Le gestionnaire VNFM utilise donc le descripteur de la VNF durant la procédure d'instanciation et pendant toute la durée de vie de la VNF. Il réalise les fonctions suivantes :

- Instancier une VNF, via une requête vers le VIM pour déclencher la création d'une instance de VNF ;
- Augmenter/réduire la capacité de traitement de la VNF (Scaling) ;
- Détruire l'instance de la VNF ;
- Consulter l'état de la VNF.

4.2.4 Système de stockage

Il existe plusieurs types de stockage utilisés par le socle :

- Un stockage commun pour les VNF et leurs données et les images des logiciels (VNF, hyperviseur).
- Une zone mémoire locale dans les nœuds de calcul. Cette mémoire locale n'est pas nécessairement disponible/utilisée sur tous les nœuds de calcul.

4.2.5 Plateforme de sécurité

La plateforme de sécurité est à l'extérieur du socle. Elle est utilisée par le socle et est gérée indépendamment par OCE dans le cadre de sa politique de sécurité.

La plateforme de sécurité est décomposée en :

1. Les composants '**Contrôle d'accès**' qui réalisent les fonctions suivantes :
    - Identification/Authentification,

- Gestion des comptes à privilèges permettant des actions d'administration,
- Gestion des rôles et des responsabilités,
- Gestion du cycle de vie des droits d'accès,
- Gestion des autorisations et des droits (création, demande, décision, etc.),
- La gestion des accès selon une démarche RBAC (Role Based Access Control),
- Un stockage sécurisé des droits d'accès sur une plateforme externe du socle (e.g. coffre-fort) et protégée dans un annuaire Idap/AD.

2. Le composant '**Gestion de déploiement**' qui réalise les fonctions suivantes :
   - Déploiement de configuration du socle,
   - Contrôle d'intégrité des fichiers de configuration de l'infrastructure,
   - Contrôle d'intégrité des fichiers de configuration des VNF
   - Contrôle d'intégrité des fichiers de configuration de la solution de virtualisation et de tous ses composants (socle),
   - Contrôle d'intégrité du code exécutable pour garantir le chargement d'un code sûr et authentique,
   - Les différentes opérations de Secure boot et contrôle d'intégrité (Hyperviseur, logiciel VIM, logiciel VNFM et VNFs) par des racines de confiance stockées sur un élément sécurisé physique (e.g. TPM).

     Note : En fonction des solutions il pourra s'avérer nécessaire de mettre en place des mécanismes assurant la confidentialité de tout ou partie des éléments de configuration.

3. Le composant '**Gestion des journaux**' qui réalise les fonctions suivantes :
   - Gestion des journaux centralisé et monitoring en temps réel au niveau hyperviseur, VNFM, VIM, VNF et communication entre VNF. Ce composant collecte les journaux des différents composants, les analyse et déclenche des actions et mesures

convenables en cas de détection d'activité anormale ou illégitimes. Les journaux sont stockés et protégés en intégrité, confidentialité, disponibilité et sont horodatées et signées pour en garantir l'authenticité,

- Gestion des journaux (traces) d'accès privilégiés. Cette gestion doit être effectuée à plusieurs niveaux : infrastructure, les composants de la solution de virtualisation et des machines virtuelles. Une sélection de journaux, expurgés des informations sensibles, doit être renvoyée vers le centre des opérations de sécurité (S.O.C.).
- Gestion des événements de sécurité. Cette gestion surveille les menaces de sécurité en temps réel pour détecter les attaques, les contenir et y répondre. Lorsqu'une attaque est lancée, ce composant fournit des données d'analyse sur tous les composants du socle (NFVI, Hyperviseur, VIM, VNFM et VNFs).

4. Le composant '**Gestion des mises à jour**' qui réalisent les fonctions suivantes :
   - Cette gestion doit être effectuée au niveau NFVI, Hyperviseur, VIM, VNFM et VNFs. Ces composants assurent que tous les logiciels et équipements sont à jour des correctifs en vigueur. Ils réalisent les mises à jour chaque fois que les fournisseurs des équipements ou logiciels émettent une mise à jour critique. Ces mises à jour peuvent être effectuées par des prestataires externes (mainteneurs, intégrateurs, etc.) exclusivement sous le contrôle de OCE.
5. Le composant '**Gestion des sauvegardes**' qui définit et applique une politique de sauvegarde afin de pouvoir établir le fonctionnement du socle suite à un incident ou à une compromission. Cette politique identifie clairement les éléments à sauvegarder, le lieu de sauvegarde et les droits d'accès qui y sont associés.

4.2.6 Gestion des clés cryptographiques

Ce composant porte sur la gestion sécurisée des clés cryptographiques utilisées par le socle. Un HSM qualifié peut être utilisé comme solution pour la protection de ces clés.

4.3 Périmètre de l'étude concernant les contraintes légales

Les contraintes légales qui s'appliquent au socle sont entre autres :

- EECC (European Electronic Communications Code) qui remplace le paquet télécom français :

  http://europa.eu/rapid/press-release_IP-18-4070_en.htm

- R226 :

  https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033063311&dateTexte=&categorieLien=id

- Les interceptions légales (IL) :

  http://igm.univ-mlv.fr/~dr/XPOSE2013/interceptions/protocoles.html

  https://www.etsi.org/technologies-clusters/technologies/lawful-interception?highlight=YToxOntpOjA7czo2OiJsYXdmdWwiO30=

- GDPR : https://www.eugdpr.org

- eprivacy :

  https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52017PC0010&from=FR

- Code des postes et des communications électroniques

  https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070987

- Code de la défense

  https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071307

4.4 Limites du périmètre

Dans le cadre de l'étude en cours nous avons convenu de limiter le périmètre de cette première version du référentiel en termes de composants, de scénarios, de contraintes légales et de sécurité à étudier.

Cette section décrit ce que nous avons décidé d'écarter dans cette première étude.

4.4.1 Composants non considérés

La figure suivante fait apparaître en grisé les composants hors périmètre de l'étude.

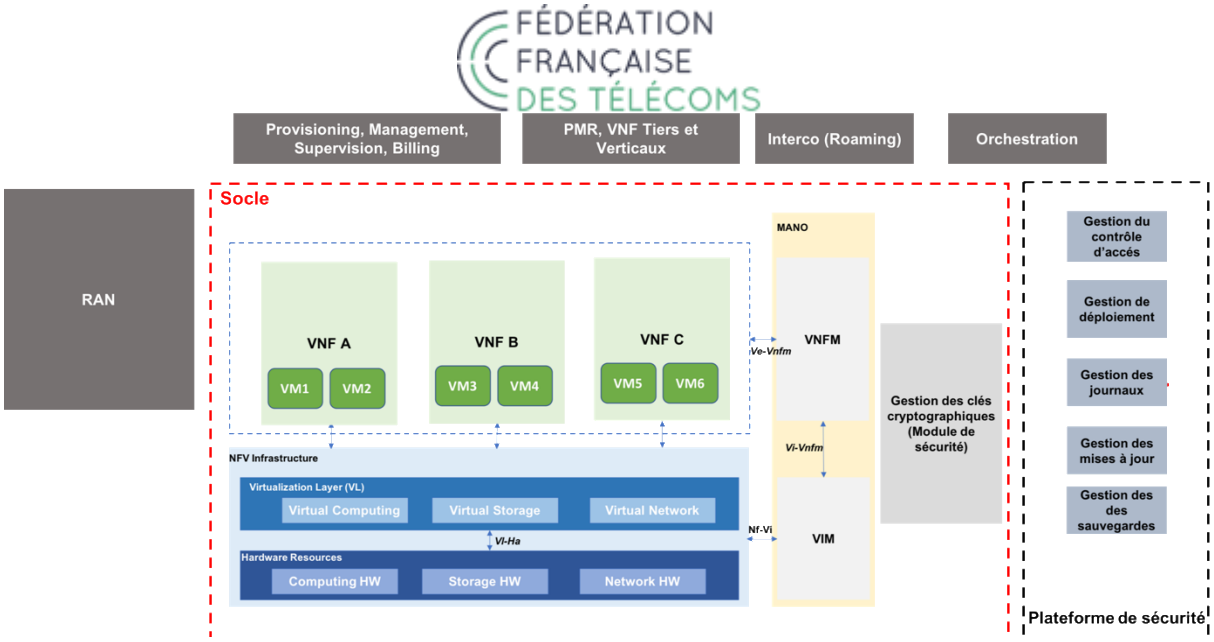

Figure 2: Les composants et les fonctionnalités hors scope

Les composants sont entre autres les suivants :

- Les réseaux d'accès radio (RAN) : La virtualisation des fonctions RAN est une des technologies clés dans le développement du système 5G. Les OCEs ont besoin de manière rentable de combiner plusieurs normes (GSM, CDMA, WCDMA, LTE, Wifi, entre autres), des bandes de fréquences, des couches cellulaires et de solutions de réseau de transport, tout en réduisant en même temps les latences et le taux de manipulation de données. Cela signifie que, avant tout, l'infrastructure cellulaire doit être souple, dynamique et peut soutenir un déploiement et une gestion simplifiée des réseaux d'accès radio de plus en plus hétérogènes.
- VNF Tiers et Verticaux (hors scope de ce document, à étudier dans une version future) : Actuellement il est prévu que les VNF fournies par des tiers soient exécutées dans une infrastructure dédiée séparée physiquement du cœur réseau. Le cœur réseau ne contiendrait que les VNF réseau. Néanmoins à terme et au cas par cas, il pourrait être envisagé une mutualisation des VNF tiers et réseau sur le même socle suite à une analyse de risque qui tiendra en compte et évaluera la sensibilité de ses VNF en fonction :
    - De la nature des informations sensibles détenues par les machines virtuelles ;
    - De la nature des fonctions virtualisées ;

  Note : Aujourd'hui, l'état de l'art ne permet pas certain niveau d'isolation ou co-localisation de VNFs réseau et tiers sur le même socle. Cependant, cela reste un thème de recherche actif qui est susceptible d'être atteint à long terme.
- Les applications et services de OCE nécessaires pour opérer les réseaux, à savoir (liste indicative) : les systèmes d'enrôlement des usagers, les systèmes de collecte des tickets de taxe et facturation, les systèmes de supervision et exploitation des logs.

- Les points d'interconnexion de la plateforme avec des systèmes distants, en particulier pour délivrer les services à des utilisateurs externes ou étrangers en 'roaming-in' sur la plateforme.
- Les systèmes d'orchestration des services délivrés aux tiers utilisant les services du socle comme ressources.

4.4.2 Contraintes légales non considérées

Les contraintes légales qui ne sont pas considérées pour cette étude sont les suivantes :

- Directive NIS (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 : Il ne porte pas sur les activités de communication électronique

  https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033122937&dateTexte=&fastReqId=293837442&fastPos=6&oldAction=rechExpTransposition

  https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L1148

- LPM (FR) : Le socle réseau n'est pas un SIIV

  https://www.ssi.gouv.fr/entreprise/protection-des-oiv/protection-des-oiv-en-france/

  https://atos.net/wp-content/uploads/2017/10/B-LPM-OIV-fr1-web.pdf

  https://www.sentryo.net/fr/oiv-obligations-loi-de-programmation-militaire/

  https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=E6CA21E5E2FF056CCDE294E9F30F64C1.tpdila12v_3?cidTexte=JORFTEXT000033521327&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000033521322%20

4.4.3 Scénarios de mutualisation non considérés

Voir chapitre 5.

5 Scénarios de mutualisation

La mutualisation est envisagée suivant plusieurs axes :

- Scénarios 1 à 5 : Mutualisation des VNF de même sensibilité dans le même socle (optimisation des ressources).
- Scénarios 6 à 9 : Mutualisation des VNF de sensibilités différentes dans le même socle. Ces scénarios sont d'actualité en terme de recherche et pourraient être envisagés :
    - Suite à une analyse des risques qui prendra en compte et évaluera les niveaux de sensibilité des VNF ;
    - Dès lors qu'un socle ou un mécanisme de virtualisation/conteneurisation ait obtenu un niveau de qualification suffisant.

  Note : Suite à une analyse des risques et à l'unique condition qu'elle démontre une isolation robuste entre les VNFs, il est envisageable de mutualiser de VNFs de sensibilités différentes sur le même socle.
- Scénarios 10 et 11 : Mutualisation de NFVI entre les différents fournisseurs des ressources matérielles et logicielles (souplesse dans la maintenance évolutive du socle et possibilité de ne pas être mono fournisseurs pour l'ensemble des composants).
- Mutualisation du module de sécurité pour la gestion des clés cryptographiques : optimisation des coûts et centralisation de l'administration des secrets.

Dans un premier temps nous considérons uniquement la mutualisation des VNF (scénarios 1 à 9) et la mutualisation du module de sécurité.

Les scénarios 10 et 11 de la mutualisation de NFVI ne sont pas traités par l'étude.

5.1 Mutualisation des VNF réseaux

Il existe une multitude de combinaisons et scénarios possibles pour la mutualisation des VNF sur un socle commun. Nous avons considéré les scénarios suivants :

Scénario	Nombre de VNF par Socle	Nombre de VNF par Nœud	Niveau de Sensibilité	Nombre de Fournisseurs par Socle	Nombre de Fournisseur par Nœud
S1	1	1	1	1	1
S2	Multiple	1	1	1	1
S3	Multiple	Multiple	1	1	Multiple
S4	Multiple	1	1	Multiple	1
S5	Multiple	Multiple	1	Multiple	Multiple
S6	Multiple	1	Multiple	1	1
S7	Multiple	Multiple	Multiple	1	Multiple
S8	Multiple	1	Multiple	Multiple	1
S9	Multiple	Multiple	Multiple	Multiple	Multiple

- **Scénario 1** :
    - Le socle héberge un ou plusieurs nœuds de calcul pour exécuter qu'une seule VNF.

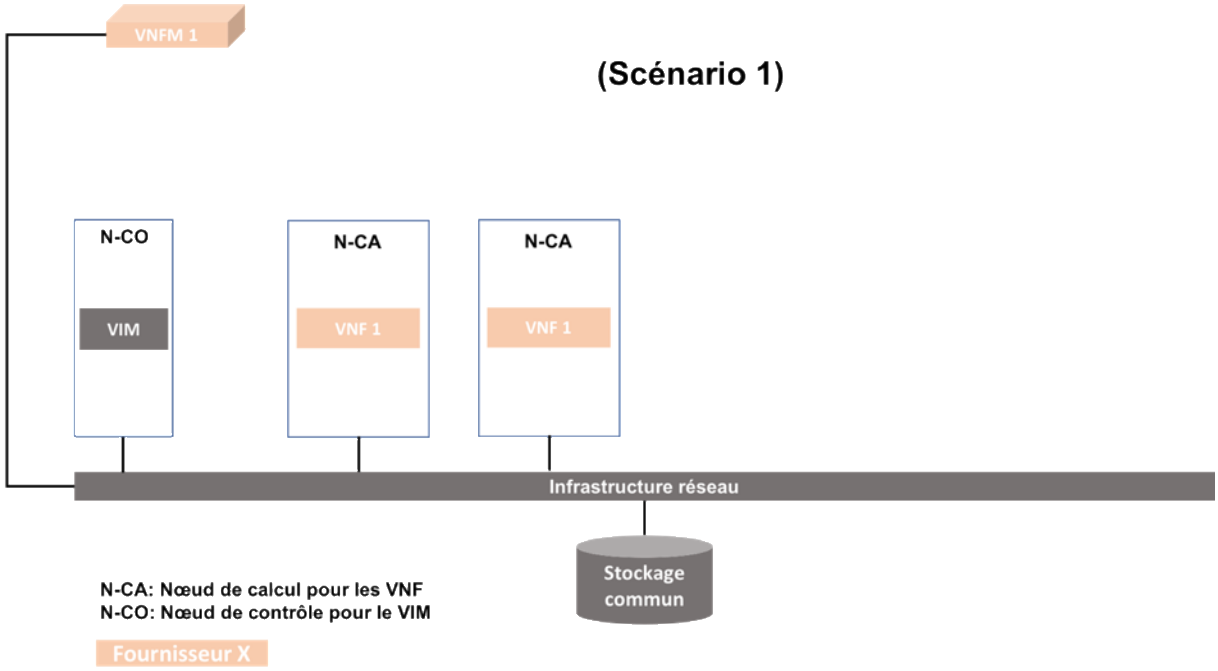

Figure 3: Scénario 1 de mutualisation

- **Scénario 2** :
    - Le socle contient plusieurs nœuds de calcul pour exécuter plusieurs VNF différentes appartenant au même fournisseur et de la même sensibilité. Chaque VNF s'exécute sur ses propres N-CA.

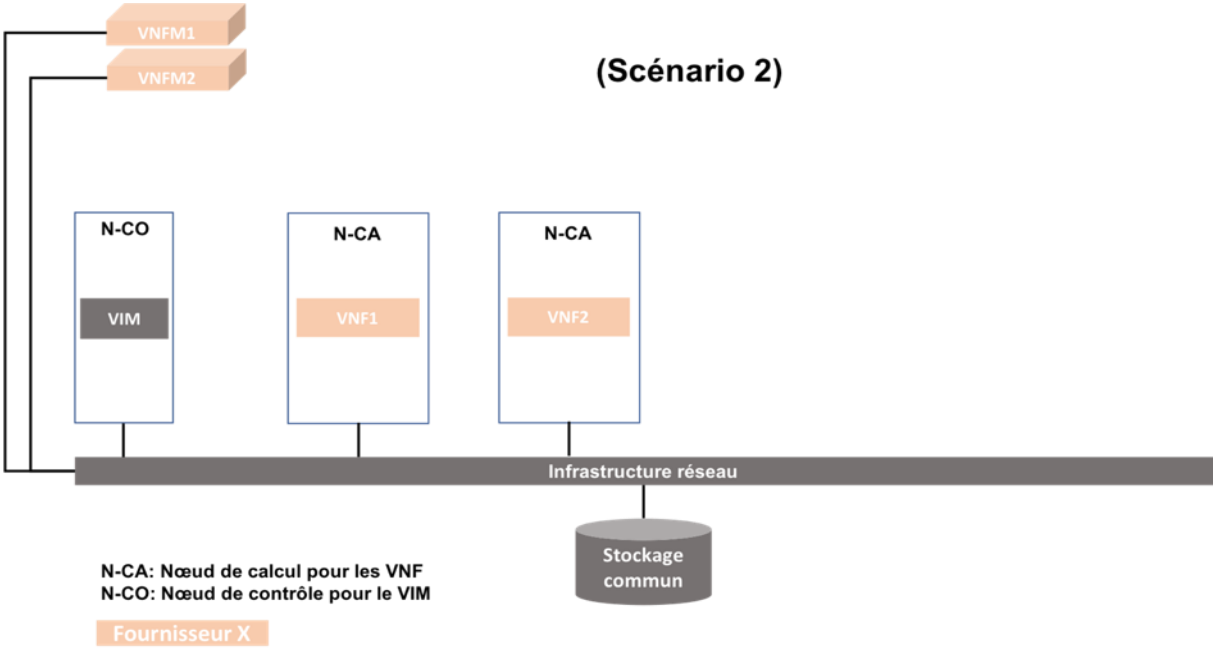

Figure 4: Scénario 2 de mutualisation

- **Scénario 3** :
    - Le socle héberge plusieurs VNF appartenant au même fournisseur, de la même sensibilité et s'exécutant sur le même N-CA.

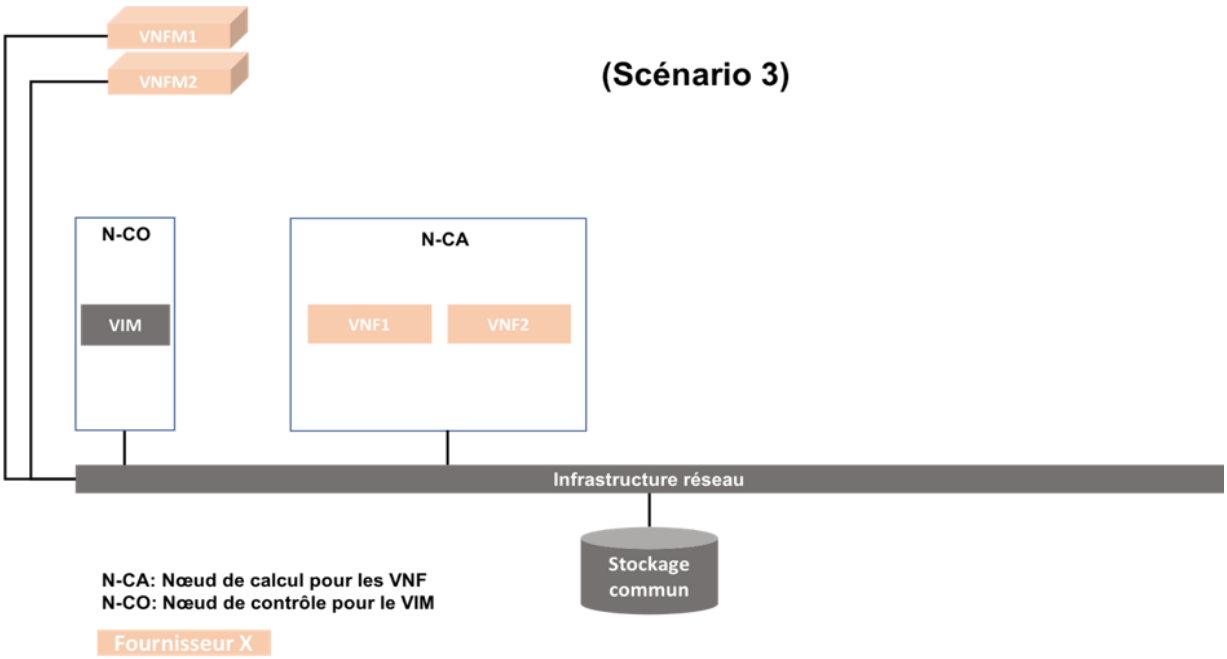

Figure 5: Scénario 3 de mutualisation

- **Scénario 4** :
    - Le socle contient plusieurs N-CA pour exécuter plusieurs VNF de même sensibilité mais de différents fournisseurs. Dans ce scénario, chaque VNF s'exécute sur ses propres N-CA.

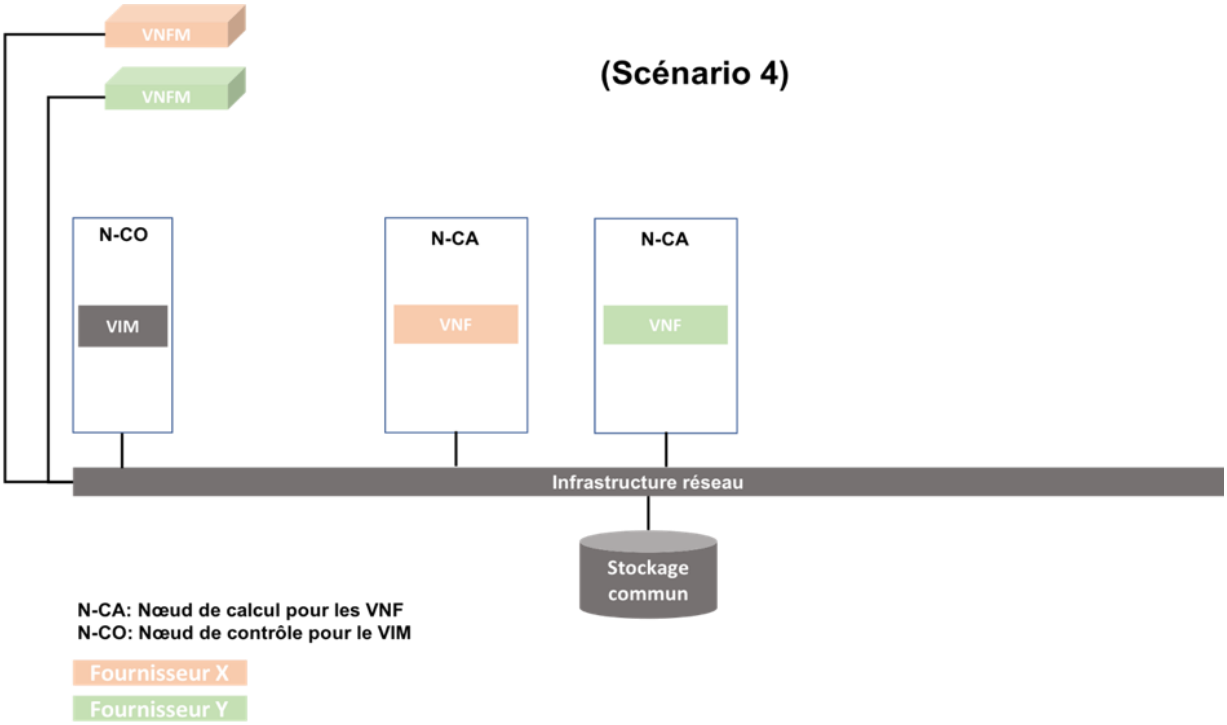

Figure 6: Scénario 4 de mutualisation

- **Scénario 5** :
    - Le socle contient un N-CA qui peut exécuter une VNF du fournisseur X et une VNF de la même sensibilité appartenant au fournisseur Y et vice versa.

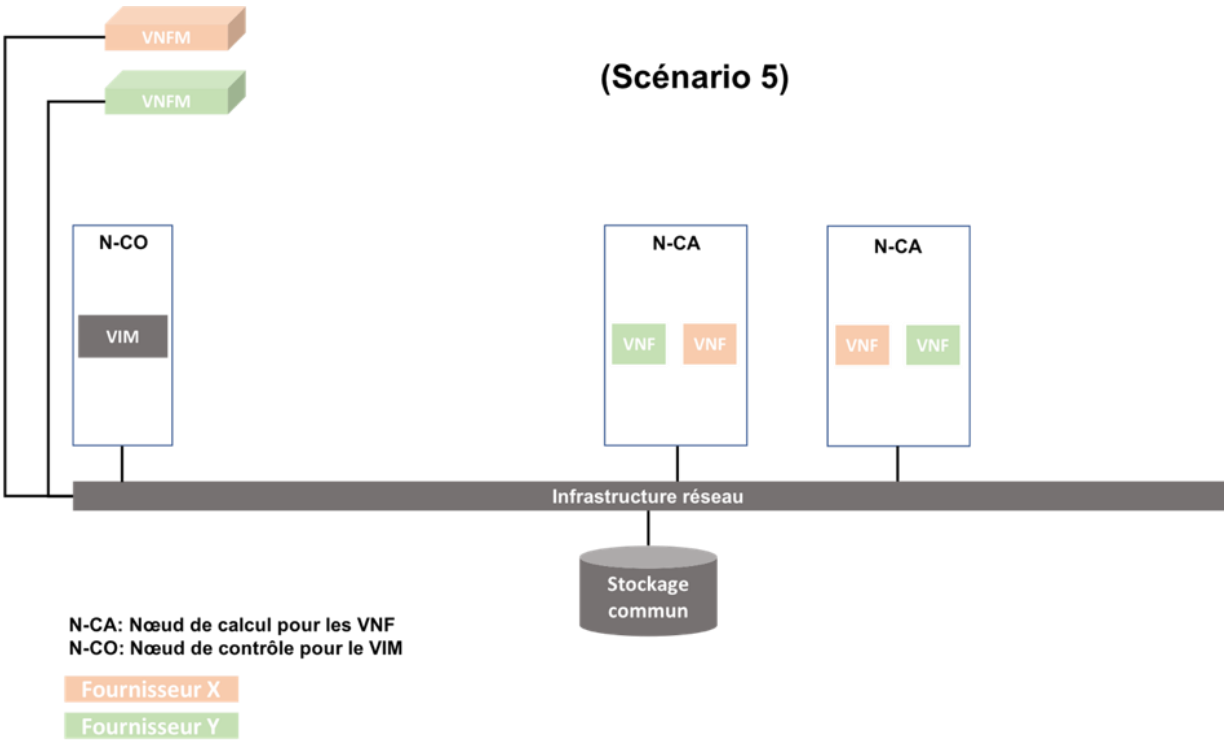

Figure 7: Scénario 5 de mutualisation

- **Scénario 6** :
    - Le socle héberge plusieurs VNF de sensibilités différentes appartenant au même fournisseur et s'exécutant sur des N-CA distincts.

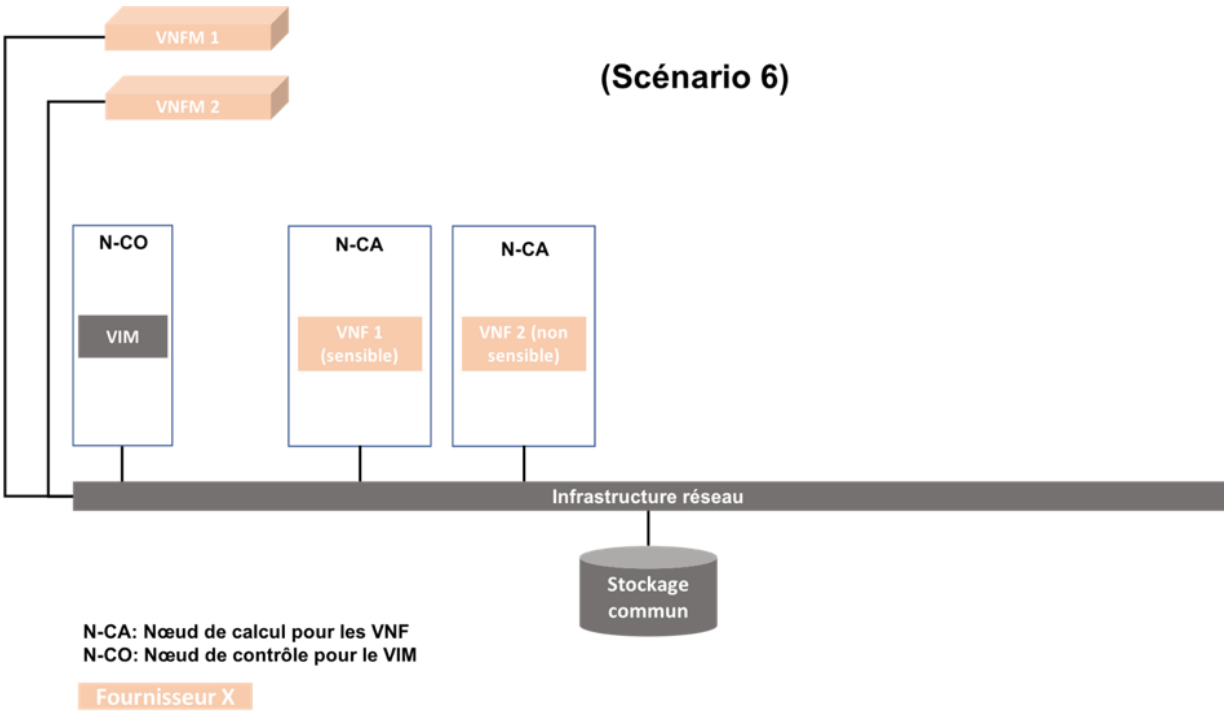

Figure 8: Scénario 6 de mutualisation

- **Scénario 7** :
    - Le socle héberge plusieurs VNF de sensibilités différentes appartenant au même fournisseur et s'exécutant sur le même N-CA.

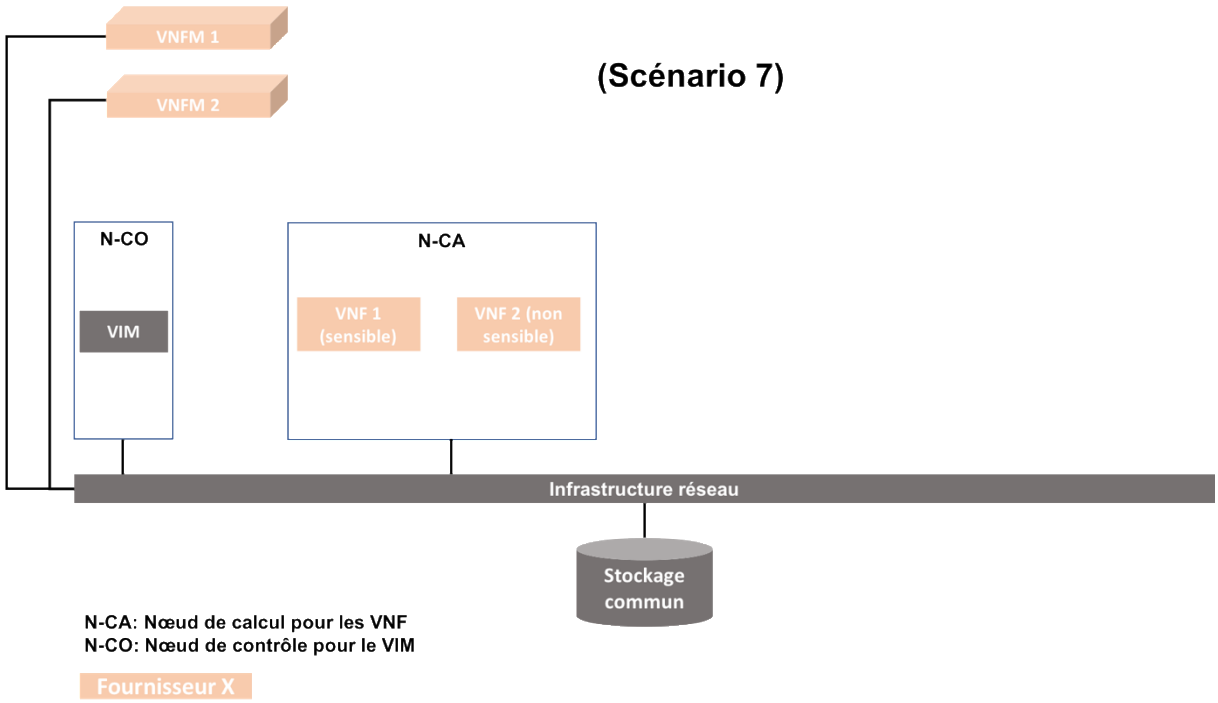

Figure 9: Scénario 7 de mutualisation

- **Scénario 8** :
    - Le socle héberge des VNF de sensibilités différentes de fournisseurs différents et s'exécutant sur des N-CA distincts.

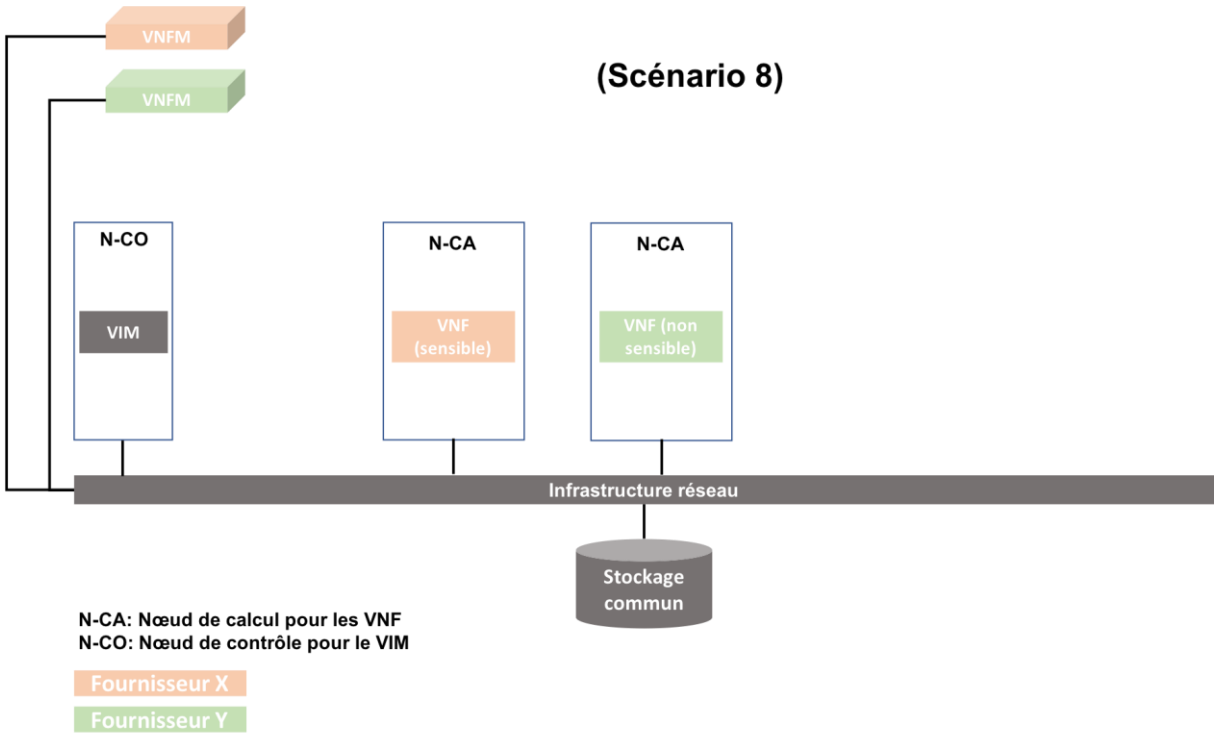

Figure 10: Scénario 8 de mutualisation

- **Scénario 9** :
  - Le socle héberge plusieurs VNF de sensibilités différentes de fournisseurs différents et s'exécutant sur le même N-CA.

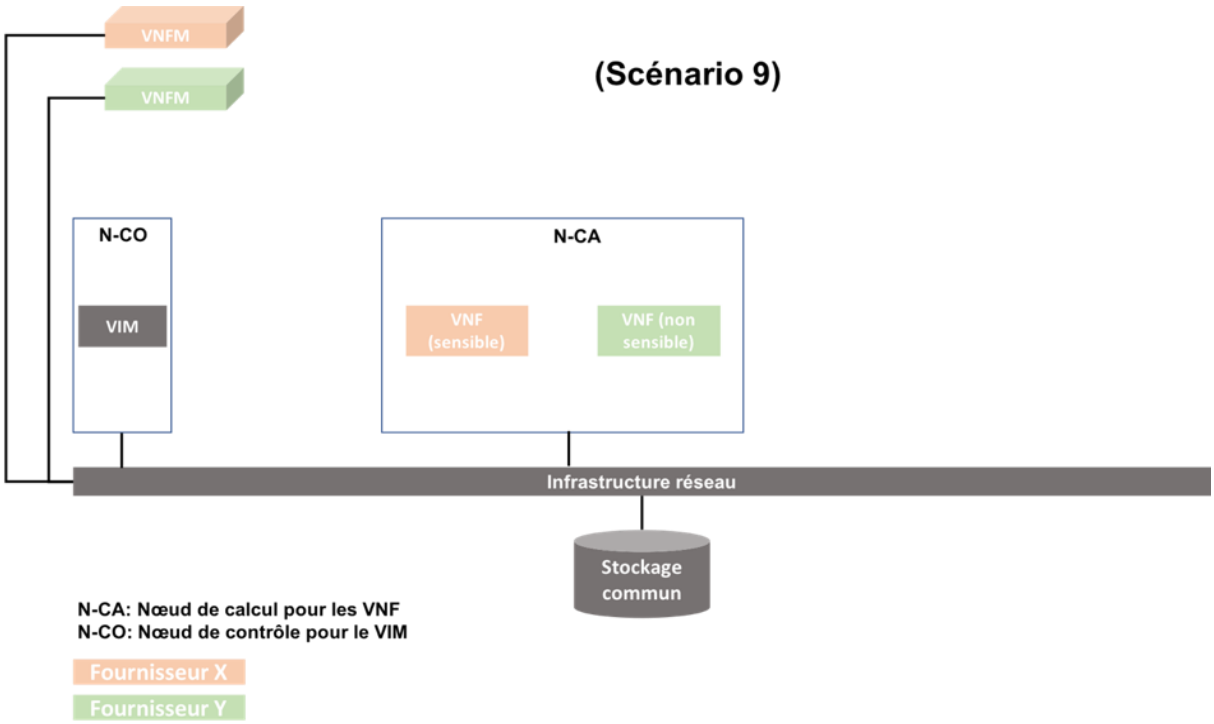

Figure 11: Scénario 9 de mutualisation

La décision dans la mise en œuvre d'un ou plusieurs scénarios va dépendre de la capacité de l'infrastructure virtualisée, l'hyperviseur, des nœuds de calcul et de contrôle d'assurer l'isolation HW et SW entre les VNF s'exécutant sur le même socle.

5.2 Mutualisation de NFVI

Les deux scénarios de cette section (10 et 11) sont donnés à titre d'exemple pour illustrer la mutualisation de nœuds de calcul dans le même socle. Ce type de scenario n'est pas exploré dans cette version du document.

- **Scénario 10** :
  - Le socle contient deux ou plusieurs N-CA de fournisseurs différents.

FÉDÉRATION FRANÇAISE DES TÉLÉCOMS

(Scénario 10)

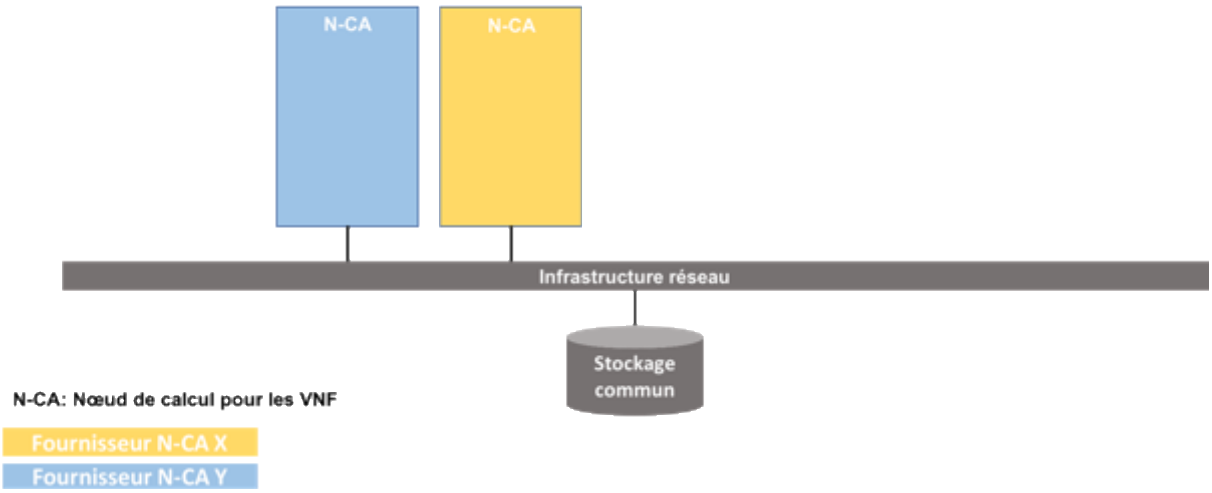

Figure 12: Scénario 10 de mutualisation

- **Scénario 11** :
  - Le socle contient deux ou plusieurs N-CA de même fournisseur mais de versions différentes.

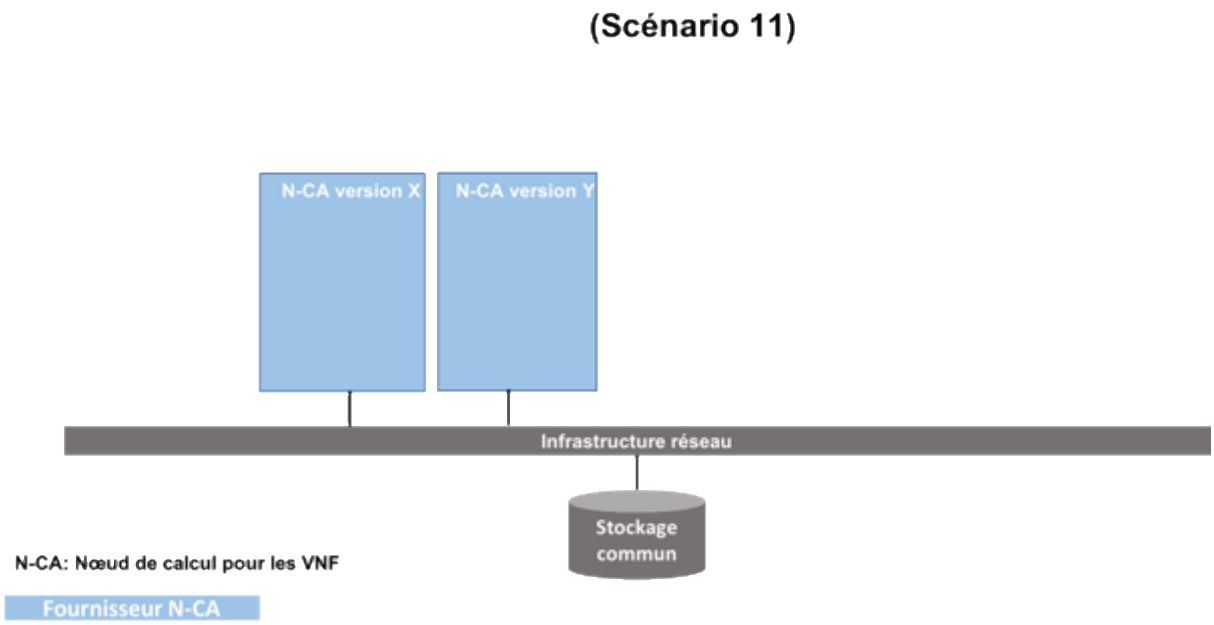

Figure 13: Scénario 11 de mutualisation

5.3 Mutualisation des modules de sécurité

Le déploiement d'un module de sécurité qualifié (par exemple un HSM qualifié) devra respecter scrupuleusement les conditions et les limites d'utilisation spécifiées dans la décision de qualification.

La centralisation et la mutualisation du module consiste à centraliser l'administration des secrets pour héberger toutes les clés cryptographiques de différents fournisseurs utilisées par le socle.

Il existe deux possibilités de mutualisation :

- Une mutualisation des ressources du module en local (même socle) – intra socle
- Une mutualisation des ressources du module entre plusieurs socles – inter socles

Pour pouvoir centraliser un module de sécurité, la protection des clés au niveau réseau est indispensable.

5.4 La mutualisation par étapes

Les objectifs à atteindre sont :

- À court terme : étude de la mutualisation des VNF de même sensibilité sur des nœuds de calcul séparés au sein du même socle (Scénario 4).

- À moyen terme : mutualiser et centraliser le module de sécurité pour héberger toutes les clés cryptographiques de plusieurs socles en mono site.
- À moyen terme : étude de la mutualisation des VNF de même sensibilité sur le même nœud de calcul au sein du même socle (Scénario 5).
- À moyen terme : étudier la mutualisation et la centralisation de plusieurs modules de sécurité qualifiés[2] (par exemple un HSM qualifié) pour héberger toutes les clés cryptographiques de plusieurs socles en multi-sites (dès lors que l'on a réussi cette mutualisation en mono site). Le déploiement et cette mutualisation ne pourront s'envisager que dans le strict respect des conditions et limites d'utilisation des produits spécifiées dans la décision de qualification.
- À long terme : étudier la mutualisation de VNF de sensibilités différentes au sein du même socle (scénarios 6 et 9).

[2] Dans la mesure où une telle solution existe

6 Prérequis

Ce chapitre liste les prérequis minimaux pour les équipements, utilisateurs et environnement physique nécessaires pour la mise en œuvre et le bon fonctionnement du socle. Les prérequis suivants doivent être considérés :

6.1 Prérequis pour l'environnement physique

- Les secrets, les matériels et les logiciels sensibles (e.g. soumis à une autorisation au titre de l'article R226-3 du code pénal) sont déployés uniquement en France.
- L'accès physique au socle par les mainteneurs et ou les équipementiers est limité à des opérations exceptionnelles. Elle est systématiquement contrôlée par les personnels autorisés de l'OCE. Toutes les opérations font l'objet d'une journalisation précise et d'un compte rendu qui peuvent être accédés de manière autonome par l'officier de sécurité et/ou le FSSI.
- L'environnement opérationnel ne permet pas à un individu non autorisé d'accéder au stockage des VNF et à ces données (physiquement ou par le réseau).
- Les serveurs physiques support de la virtualisation sont installés dans des locaux sécurisés disposant d'une authentification à double facteur et à minima d'un contrôle d'accès par badge disposant d'un visa de sécurité. Les journaux de logs sont exportés en temps réel vers un serveur de Log sécurisé. Les journaux de logs sont conservés pendant un an.
  Note : Ce prérequis n'est pas aujourd'hui pris en compte pour les équipements physiques actuels. Une investigation à moyenne terme est prévue par les OCEs.
- La racine de confiance utilisée pour assurer le démarrage sécurisé de l'hyperviseur est protégée dans un élément sécurisé (e.g. HSM, TPM) qualifié[3].
- Les clés cryptographiques sont protégées et stockées dans un module de sécurisé (par exemple HSM) qualifié[4].
- Les secrets d'authentification et de chiffrement sont protégés et stockés dans un coffre-fort numérique[5].
- L'environnement opérationnel ne permet pas à un individu non autorisé d'accéder aux baies informatiques dans lesquelles le socle est installé.
- Tous les outils logiciels, équipements et matériels nécessaires à l'installation, configuration et à l'opération du socle sont intègres, sains, à jour des correctifs en vigueur au moment de l'installation exempts de virus, etc.
- Sur les postes de travail sensibles, sur lesquels sont par exemple manipulés des comptes à privilèges de l'annuaire Active Directory, la sécurité doit être assurée afin d'atténuer les risques d'élévation de privilèges des attaquants.

[3] Dans la mesure où une telle solution existe.
[4] Dans la mesure où une telle solution existe.
[5] Dans la mesure où une telle solution existe.

Les contremesures physiques et organisationnelles sont hors scope et ne sont pas détaillées dans ce document.

6.2 Prérequis pour les équipements

Les prérequis minimaux sur les matériels et logiciels utilisés dans le socle sont les suivants :

6.2.1 Prérequis de sécurité dans les appels d'offre

- Les prérequis en matière de sécurité concernant les équipements et les logiciels (e.g. VNF) sont intégrés par l'OCE dans les appels d'offres. La réponse technique et analyse de sécurité du fournisseur sont transmises préalablement aux audits de sécurité.
- Les OCEs doivent être les seuls à disposer d'un compte de haut niveau (par exemple root, super utilisateur, administrateur de sécurité etc.) permettant d'accéder de manière autonome aux paramètres appartenant aux OCEs nécessaires pour l'exploitation des composants matériels et logiciels du socle.
- Tous les journaux de quelque nature que ce soit doivent être accessibles en clair ou déchiffrable par les OCEs.
- Tous les accès locaux et à distance des dispositifs matériels et logiciels sont exclusivement effectués au moyen d'une solution assurant l'authentification nominative, ainsi que la confidentialité et l'intégrité des échanges. Les solutions retenues sont conformes à l'état de l'art. Il est fortement recommandé que tous les accès soient effectués en utilisant un certificat appartenant aux OCE.
- Les opérations d'administration ne doivent jamais être effectuées depuis des interfaces accessibles à partir du réseau public ou depuis un quelconque réseau externe au réseau de l'OCE.
- Les dispositifs matériels et logiciels doivent être munis d'un dispositif de filtrage local. Ce dernier doit pouvoir être mis en œuvre sur toutes les interfaces.
- Les core dump doivent être exempts de toutes données sensibles.

6.2.2 Prérequis matériels

- Les équipements matériels (e.g. nœuds de calcul) respectent les exigences qui permettent à l'OCE d'atteindre les prérequis du présent référentiel.
- Les équipementiers réalisent une analyse de sécurité de leurs produits. Ils fournissent le rapport à l'ANSSI.
- Une liste exhaustive des comptes, des mots de passe et des certificats par défaut sont transmis à l'OCE. Elle est accompagnée de la procédure permettant de les modifier avant passage en production.
- Aucune clé ou certificats utilisés pour la réalisation d'actions d'administration des services sensibles ne doit être présent dans le code.
- Les matériels doivent en matière de sécurité être conformes à l'état de l'art.
- Tous les matériels doivent accepter les certificats et les autorités de certification des OCEs.

6.2.3 Prérequis logiciels

- Une analyse de sécurité est réalisée par les équipementiers sur leurs logiciels. Le rapport de l'analyse de sécurité détaillé est communiqué à l'ANSSI.
- Les logiciels (Hyperviseur, VIM, VNFM et VNF) sont analysés et testés par les OCEs. Dans le cadre d'une mise en service ou d'une maintenance de sécurité majeure du socle, les OCEs réalisent une analyse de sécurité et partage les résultats nécessaires en matière de sécurité avec l'ANSSI.
- Une liste exhaustive des comptes et des mots de passe par défaut sont transmis à l'OCE. Elle est accompagnée de la procédure permettant de les modifier avant passage en production.
- Aucune clé et ou certificats utilisés pour la réalisation d'actions d'administration sensibles ne doit être présent dans le code.
- Tous les logiciels doivent accepter les certificats et les autorités de certification des OCEs.
- Les logiciels doivent en matière de sécurité être conformes à l'état de l'art.

6.3 Prérequis Utilisateurs

6.3.1 Administrateur

- Les administrateurs agissent sous la responsabilité de l'OCE.
- Les administrateurs respectent les procédures décrites dans les guides fournis par les OCEs et les fournisseurs.
- Les administrateurs sont sensibilisés aux bonnes pratiques en matière de sécurité (règles sur la qualité des mots de passe ou phrases secrètes, règles permettant d'éviter la compromission de ces secrets, etc.).
- Les administrateurs de sécurité sont chargés de la conservation dans un lieu sûr des clés cryptographiques, et de la non divulgation des droits d'accès.

6.3.2 Mainteneur

- Les prestataires externes, les mainteneurs et les intégrateurs agissent exclusivement sous la responsabilité de l'OCE dans le cadre d'un contrat fournisseur-OCE.
- Les prestataires externes, les mainteneurs et les intégrateurs du socle sont compétents et formés pour la configuration et la mise à jour des VNF. Ils agissent exclusivement sous le contrôle de l'OCE.
- Les prestataires externes, les mainteneurs et les intégrateurs respectent les procédures décrites dans les guides fournis par les OCEs et les fournisseurs ainsi que les recommandations publiées sur le site de l'ANSSI (à la date de rédaction de ce référentiel www.ssi.gouv.fr).
- Les mainteneurs et les prestataires externes sont sensibilisés aux bonnes pratiques en matière de sécurité.

- Les mainteneurs et les prestataires externes doivent disposer de leur propre infrastructure d'administration sous la responsabilité de l'OCE.

6.3.3 Opérateur de communications électroniques (OCEs)

- Les OCEs doivent disposer de leur propre infrastructure de gestion de clés et de leur propre autorité de certification. Les OCEs déploient dans les matériels et dans les logiciels mis en production lorsque c'est possible leur propre certificats et autorité de certification.
- Les OCEs doivent mettre en place une politique de droits et de permissions respectant strictement le besoin d'en connaître. Ils doivent en conséquence analyser commande par commande les permissions affectées à chaque rôle en s'assurant qu'une élévation triviale de privilège n'est pas possible.
- Tous les outils logiciels, équipements et matériels nécessaires à l'installation, configuration et à l'opération du socle doivent être intègres, sains et à jour de leurs correctifs de sécurité.
- Les équipements (nœuds de calcul, routeurs, commutateurs, etc.) et les logiciels (VNF, etc.) du fournisseur sont testés et paramétrés correctement par l'OCE avant la mise en service.

6.4 Prérequis en matière de déploiement

6.4.1 Administration des dispositifs

Voir objectifs 5 et 6.

6.4.2 Exploitation des dispositifs

Il est indispensable de déterminer les applicatifs et fonctions les plus exposés aux risques en matière d'atteinte à la disponibilité du réseau ou à la confidentialité des données des abonnés. Cette analyse de risque doit être menée dans tous les projets de déploiement et plus particulièrement dans le cas de la virtualisation.

Dans le cas particulier des déploiements liés aux technologies 5G, il est envisagé, en l'état de la standardisation, d'ouvrir le réseau à des VNF de nouveaux acteurs non équipementiers. Cette situation engendrera des nouveaux risques et il conviendra de mettre en place un cloisonnement strict entre ces nouvelles VNFs tierces et les cœurs des réseaux. Les OCEs doivent s'assurer de l'innocuité des VNF de tiers candidates à la mise en production, par rapport à la sécurité globale de leurs infrastructures et aux VNF réseaux ou de tiers déjà en opération.

6.4.3 Disponibilité

Voir objectif 14.

6.4.4 Journalisation

La collecte des journaux d'événements doit être centralisée. Les informations transmises au SOC (alarmes et journaux) sont filtrées et expurgées de toutes informations sensibles. Elles peuvent être consolidées sur un système unique.

6.4.5 Sauvegarde

Voir objectif 19 et contremesure 23.

6.4.6 Mises à jour

Voir objectif 15.

6.4.7 Gestion des licences

Il est fortement déconseillé aux OCEs de raccorder leurs réseaux de quelque manière que ce soit en temps réel à un réseau d'un prestataire interne ou externe ou d'un équipementier.

6.4.7.1 Serveurs de gestion des licences

Les solutions mises en œuvre par les équipementiers afin de contrôler les fonctionnalités déployées par les OCEs ne doivent jamais être raccordées à un dispositif externe aux réseaux des OCE (par exemple Internet, ou un intranet d'un équipementier). De plus, l'activation d'une licence doit impérativement être effectuée par un OCE et à minima sous son entière responsabilité. Tous les éléments techniques liés à l'activation d'une nouvelle fonctionnalité doivent être conservés et tracés. Ils doivent notamment permettre d'identifier :

- Nominativement le responsable de l'opération (équipementier et OCE) ;
- La nature exacte des évolutions ;
- Les éléments techniques liés à l'opération (date, compte d'administration utilisé, procédure, interface technique, protocole, etc.) ;
- Les journaux liés à l'installation et à l'activation des fonctionnalités ;
- Il serait recommandé que l'OCE conserve une copie des logiciels, codes, fichiers liés aux évolutions.

Note : lorsque la solution de gestion des licences permet d'activer des fonctionnalités de nature à permettre l'atteinte au secret des correspondances (par exemple mais liste non exhaustive : la fonction interception, SIP-REC, analyse fine du data plane, etc.), le dispositif doit obtenir une autorisation au titre de l'article R226-3 du code pénal par le Premier ministre (par délégation l'ANSSI en France).

6.4.7.2 Contrôles des licences et des performances

Les équipementiers souhaitent parfois vérifier que les fonctionnalités mises en œuvre par les OCEs correspondent aux fonctionnalités acquises contractuellement par ces derniers. Les équipementiers se réservent donc la possibilité de réaliser des audits afin de contrôler la conformité de l'utilisation des logiciels au regard des clauses contractuelles.

Il convient toutefois, que de tels audits de licences ou de capacités ne soient effectués que par les OCEs. Les OCEs doivent donc disposer des modalités pratiques liées à la réalisation de ces audits et ils doivent impérativement connaître les commandes ou opérations liées à ces audits, disposer des droits pour effectuer ces opérations et être en mesure d'interpréter les résultats des audits avant de les transmettre aux équipementiers.

6.4.8 Génération des secrets

Voir objectif 8.

6.4.8.1 Mise en place d'une PKI OCE

Voir objectif 8.

6.4.8.2 Utilisation d'un module de sécurité

Voir objectif 8 et contremesure 8.

6.5 Prérequis pour la communication des informations entre les parties

Dans ce document nous faisons l'hypothèse que les rapports d'audit et les résultats des tests réalisés sur les équipements des fournisseurs et les infrastructures des OCEs sont disponibles pour construire l'analyse de sécurité selon ce référentiel. Cette analyse peut être conduite par OCE, par un tiers accrédité par l'ANSSI ou bien directement par l'ANSSI.

Ceci implique que les contrats qui lient les parties (fournisseurs, auditeurs de sécurité et OCEs) permettent explicitement la transmission de des rapports complets[6] (les rapports d'audit et résultats de tests) à l'ANSSI et à tout tiers autorisé (PASSI, CESTI, etc.) accrédité par l'ANSSI.

Cette disposition a pour but de rendre les analyses de sécurité plus efficaces en favorisant la réutilisation des analyses déjà faites.

[6] La communication de ces informations ne peut être envisagée sans le strict respect de la propriété intellectuelle de chacun.

7 Utilisateurs

La liste des utilisateurs susceptibles d'interagir avec le socle ainsi leurs rôles sont présentés dans le tableau suivant. La dernière colonne distingue les acteurs agissant sous la responsabilité :

- Directe de l'OCE ou
- Fournisseurs ou Tiers agissant dans le cadre d'un contrat avec l'OCE.

Acteurs	Rôles	Operateur, Fournisseur, Abonnés, Tiers
Administrateur sécurité	Il peut auditer tous les composants du système et créer ou supprimer des comptes utilisateurs pour n'importe quel rôle. Il gère les coffres forts qui stockent les identifiants des autres administrateurs. Il peut modifier tous les mots de passe. C'est le détenteur du mot de passe racine et de la clé racine du chiffrement des secrets. Il gère la configuration de sécurité des composants : configuration des droits d'accès, mécanisme de stockage des mots de passe et des clés cryptographiques, paramètres IPSec, positionnement des secrets, mots de passe, clés et certificats, configuration des mécanismes d'accès distant, etc.	OCE
Administrateur système	Il administre les composants « systèmes » (à titre d'exemple : sauvegarde, mise à jour, configuration des journaux systèmes, de la synchronisation temporelle, Taxe / provisioning (détails des communications) en particulier s'interface avec le HSS (e.g. UDM en 5G)). Il est bien formé sur la confidentialité des communications, etc.).	OCE
Administrateur de fonctions sensibles	Il administre les composants « sensibles » de l'équipement (à titre d'exemple fonction interception, etc.).	OCE
Exploitants de fonctions sensibles	Il exploite les composants « sensibles » de l'équipement (à titre d'exemple fonction interception, etc.).	OCE
Administrateur VNF	Il peut configurer la fonction réseau portée par l'équipement. Il gère les fonctions réseau. Il peut réaliser les tâches d'exploitation quotidienne (notamment le provisioning) de la fonction réseau VNF.	OCE
Administrateur VIM	Il gère les activités du VIM. Il peut configurer le VIM porté par l'équipement. Il peut réaliser les tâches d'exploitation quotidienne (notamment le provisioning) du VIM porté par l'équipement. Il contrôle les fonctions permettant d'accéder au VIM. Il est en charge de réaliser la configuration matérielle des VNF.	OCE
Administrateur VNFM	Il gère les activités du VNFM. Il peut configurer le VNFM porté par l'équipement. Il peut réaliser les tâches d'exploitation quotidienne (notamment le provisioning) du VNFM porté par l'équipement. Il contrôle les fonctions permettant d'accéder au VNFM.	OCE
Administrateur de la couche de virtualisation (Hyperviseur)	Il gère la couche de virtualisation (Hyperviseur). Il peut configurer la couche de virtualisation portée par l'équipement. Il peut réaliser les tâches d'exploitation quotidienne (notamment le provisioning) de la couche de virtualisation portée par l'équipement. Il contrôle les fonctions permettant d'accéder à cette couche.	OCE
Administrateur des nœuds de calcul (serveurs physiques)	Il gère les nœuds de calcul (serveurs physiques). Il peut accéder à la console graphique du nœud, démarrer, arrêter, redémarrer le nœud. Il peut activer/désactiver les interfaces réseau du nœud et consulter l'état du celui-ci. Il gère le stockage local dans les nœuds de calcul.	OCE
Administrateur du réseau physique	Il gère les équipements du réseau physique (Switch, Routeurs, etc.)	OCE
Administrateur de stockage	Il gère le stockage commun	OCE
Administrateur module de sécurité	Il gère le stockage des secrets sensibles (les clés IL, les clés VNF et hyperviseur, etc.) dans les modules de sécurité.	OCE
Mainteneur (fournisseur ou tiers)	Il peut accéder à distance (via VPN par exemple) ou en local aux équipements pour mettre à jour, paramétrer, supprimer ou ajouter des applications réseau. Il a accès aux interfaces de configuration des nœuds de calcul pour la mise à jour des Firmware et la configuration des fonctionnalités BIOS, CPU, MMU, etc. Le mainteneur intervient sur le socle sous le contrôle de l'OCE qui (via par exemple IAM : Identity Access Management) lui crée des comptes spécifiques pendant une durée spécifique.	Fournisseur ou Tiers
Technicien de maintenance sur site	Il a comme tâche le raccordement et le brassage des équipements Hardware (e.g. Switch, routeurs) afin de permettre aux différents administrateurs et opérateurs de paramétrer le socle.	OCE

Laboratoire de validation interne	Il s'occupe des qualifications fonctionnelles, patchs, sécurité/conformité des applications réseaux, configurations etc. pendant tout le cycle de vie du socle.	OCE
Intégrateurs de la couche de virtualisation (Hyperviseur), VIM, VNFM et VNF	Ils réalisent uniquement l'intégration, l'installation et la configuration initiale de chaque composant de la couche de virtualisation (Hyperviseur), VIM, VNFM et VNF	OCE
Intégrateur du matériel	Ils réalisent uniquement l'intégration, installation et la configuration initiale du matériel	OCE
Utilisateurs (abonnés) du service virtualisé	Ces utilisateurs ont un abonnement et peuvent donc accéder aux services virtualisés. Lorsqu'ils accèdent à un service, ils génèrent directement ou indirectement un flux de données au sein du plan de contrôle, puis du plan usager. Leurs communications sont transportées par le plan usager.	Abonné

Table 1 Liste des Utilisateurs

8 Biens

Les services offerts par le socle doivent être disponibles et intègres. Par ailleurs, des mécanismes doivent aussi protéger les données ci-dessous. Pour chaque donnée sensible, leur détenteur et leurs propriétés de protection sont précisés dans le tableau suivant.

Suivant la conception des dispositifs la confidentialité et ou l'intégrité pourrait ne pas être nécessaire. Une analyse au cas par cas est donc impérativement nécessaire.

Par ailleurs, les informations sensibles doivent être séparées des fichiers de configuration et des journaux indispensables à l'exploitation des dispositifs. Il en est de même pour certaines informations sensibles liées à la configuration de fonctions sensibles qui ne doivent être connues que d'une certaine catégorie d'administrateur (par exemple fonction interception, données personnelles, informations bancaires etc.).

Données	Description	Détenteur	Confidentialité	Intégrité	Authenticité	Disponibilité	Privacy
Droits d'accès							
Droits d'accès – VNF sensible	Les droits d'accès des administrateurs qui ont accès aux VNF sensibles (leurs mots de passe, autorisation administrative, etc.)	Administrateur sécurité	X	X	X	X	
Droits d'accès – Socle	Les droits d'accès des administrateurs du socle (Hyperviseur/OS, VIM, VNFM)	Administrateur sécurité	X	X	X	X	
Droit d'accès réseau	Les droits d'accès des administrateurs qui ont accès au réseau physique (switch, routeur, etc.) (leurs mots de passe, autorisation administrative, etc.)	Administrateur sécurité	X	X	X	X	
Clés cryptographiques							
Clé racine	La clé racine de l'administrateur sécurité	Administrateur sécurité	X	X	X	X	
Mot de passe racine	Le mot de passe racine de l'administrateur sécurité	Administrateur sécurité	X	X	X	X	
Clés privées – communication sécurisée	Les clés privées pour initier les communications sécurisées entre VNF (e.g. Clés IPSec/TLS)	Administrateur sécurité	X	X	X	X	
Clés de chiffrement – VNF sensible	Les clés de chiffrement/déchiffrement des exécutables des VNF et ses données.	Administrateur sécurité	X	X	X	X	
Clés de chiffrement des volumes et des images	Les clés cryptographiques gérées par l'hyperviseur pour le chiffrement des volumes et des images	Administrateur sécurité	X	X	X	X	

Certificats	Les clés d'authentification privée/publique spécifiques à chaque VM : 1. Une clé privée permettant à une VM de s'authentifier auprès des autres VM 2. Une clé publique (ou d'un ensemble de clés publiques) permettant à une VM d'authentifier les données reçues par une autre VM	Administrateur sécurité	X (Que pour les clés privées)	X	X	X	
Clé boot	Une clé utilisée pour assurer un boot sécurisé	Administrateur sécurité	X	X	X	X	
Administration							
Administration	Serveurs d'administration, OSS équipementiers, Passerelle de rebond, Clients d'administration, Poste d'administration	Administrateur système				X	
Flux et interfaces							
Flux de commandes	Les flux de commandes et les paramétrages / configurations des VNF, VIM, VNFM et Hyperviseur/OS	NA	X	X	X		
Flux de données	Les flux transitant par le socle. Le socle ne doit pas altérer de manière illicite ces flux et ne doit pas permettre à une personne, un équipement ou logiciel non explicitement autorisé de les altérer. De façon symétrique, le socle ne doit pas être perturbé ou altéré (données, services, disponibilités) par les flux reçus des abonnés/clients.	NA	X	X	X		
Interfaces VNF	Trafic transitant sur les interfaces internes inter VM et externes avec le réseau physique et le stockage commun.	Administrateur VNF	X	X	X	X	
Interfaces VNFM	Trafic transitant en interne dans le VNFM et sur les interfaces externes avec les VNF et le VIM	Administrateur VNFM	X	X	X	X	
Interfaces VIM	Trafic transitant en interne dans le VIM et sur les interfaces externes avec les VNFM et la couche de virtualisation (Hyperviseur)	Administrateur VIM	X	X	X	X	
Interfaces couche de virtualisation	Trafic transitant en interne et sur les interfaces externes avec le VIM et les VNF	Administrateur couche de virtualisation (Hyperviseur)	X	X	X	X	
Interfaces des fonctions sensibles	Trafic lié au fonctionnement des fonctions sensibles	Administrateur et exploitants des fonctions sensibles	X	X	X	X	
Données abonnés							
Données des Abonnés	Identité, données de souscription et crédential abonné	Administrateur système	X	X	X	X	X
Journaux							
Journaux – accès aux nœuds de calcul	Le socle ne doit pas permettre à une personne, équipement ou logiciel de supprimer ou modifier des journaux s'il n'en a pas explicitement les droits. La durée de vie avant la destruction des journaux est au minimum de 3 mois.	Administrateur des nœuds de calcul (serveurs physiques)	X	X	X	X	

Journaux – accès aux équipements du réseau physique		Administrateur du réseau physique	X	X	X	X	
Journaux – accès aux interfaces de gestion et configuration du socle		Administrateurs VIM, VNFM et couche de virtualisation (Hyperviseur)	X	X	X	X	
Journaux – opérations en temps réel		Administrateur système	X	X	X	X	
Journaux – systèmes d'exploitation		Administrateur système	X	X	X	X	
Journaux – activités administratives		Administrateur système	X	X	X	X	
Journaux – comportement des VNF		Administrateur VNF	X	X	X	X	
Journaux – comportement des hyperviseurs, VIM et VNFM		Administrateurs VIM, VNFM et couche de virtualisation (Hyperviseur)	X	X	X	X	
Journaux de délivrance, basculement, etc.		Administrateur système	X	X	X	X	
Journaux – Accès au stockage commun		Administrateur de stockage	X	X	X	X	
Journaux – Comportement des modules de sécurité		Administrateur module de sécurité	X	X	X	X	
Code, disques et données							
Logiciel et code	Les logiciels et les code source des composants suivants : Hyperviseur/OS, VIM, VNFM et VNF	Administrateurs VNF, VIM, VNFM et couche de virtualisation (Hyperviseur)	X	X	X	X	
Données de configuration	Données de configuration des composants suivants : Hyperviseur/OS, VIM, VNFM et VNF	Administrateurs VNF, VIM, VNFM et couche de virtualisation (Hyperviseur)	X	X	X	X	
Données de configuration	Données de configuration des fonctions sensibles	Administrateur des fonctions sensibles	X	X	X	X	

Données – VNF	Données des VNF hébergées dans le système de stockage commun, la RAM et le disque dans le nœud de calcul Fichiers de description des VNF Liste des VNF autorisées	Administrateur VNF	X	X	X	X	

Table 2 Liste des Biens

9 Menaces

Cette section présente les différentes menaces liées à la virtualisation dans le socle. Les menaces présentées permettent d'obtenir un accès privilégié aux fonctions/informations manipulées par une VNF (c'est-à-dire de rompre l'isolation entre les composants mis en œuvre par la virtualisation).

L'analyse des menaces sur la virtualisation dans le socle est basée sur les informations collectées pendant les entretiens avec les OCEs ainsi que le document ANSSI 3326.

9.1 Agents menaçants

Les agents menaçants considérés dans l'étude sont les suivants :

- Une personne (interne ou externe) ayant un accès logique ou physique à des équipements pouvant se connecter au socle mais ne disposant pas d'autorisation.
- Les administrateurs sous le contrôle de l'opérateur ou d'un tiers (voir Chapitre 7) ayant obtenus un accès illégitime au socle.
- Les administrateurs ou les opérateurs internes malformés ayant un accès légitime au socle.
- Les administrateurs ou les opérateurs internes malveillants ayant un accès légitime au socle.
- Les administrateurs ou les opérateurs internes ayant un accès légitime au socle mais ne disposant pas d'autorisation.
- Les opérateurs internes ayant obtenus un accès illégitime au socle.
- Les fournisseurs d'équipements (développeur, intégrateur, etc.) malformés ou corrompus ayant un accès légitime au socle.
- Les mainteneurs (fournisseur ou tiers) malformés ou corrompus ayant un accès légitime au socle.
- Les utilisateurs (clients/abonnés) des services de la plateforme, par injection de paquets spécifiques pour perturber le plan de contrôle ou le plan usager.
- Les interfaces et accès externes au socle

9.2 Menaces applicables au socle

9.2.1 Catégories de menaces

Les catégories de menaces prises en compte sont les suivantes :

- Services
  - Disponibilité du service ou des équipements
  - Fonctionnement d'un service ou d'un équipement virtualisé ou non virtualisé
  - Authentification mutuelle entre fonctions virtualisées, couche matérielle, hyperviseur, VIM et VNFM (localisation des fonctions virtualisées, contrôle d'intégrité, journalisations des évènements)

- Informations (Liste des biens dans le chapitre 8)
  - Confidentialité des informations enregistrées en mémoire ou transitant sur le réseau qu'il soit virtuel ou non virtuel
  - Intégrité des informations enregistrées en mémoire ou transitant sur le réseau qu'il soit virtuel ou non virtuel
- Actions/Opérations
  - Imputabilités des actions et des évènements se produisant au sein de la solution virtualisée (plateforme matérielle, couche de virtualisation et fonctions virtualisées)
  - Légitimité des opérations réalisées par ou sur les plateformes virtualisées

9.2.2 Disponibilité

Les menaces affectant la disponibilité des équipements et/ou des services sensibles virtualisés sont de deux types :

1. **Type 1** : Les menaces résultant d'un déni de service par une surcharge du réseau (signalisation ou trafic) ou altération du trafic du réseau (par des injections, du rejeu de trame, du fuzzing sur des paramètres spécifiques, etc.) nécessaire au fonctionnement du service.
2. **Type 2** : Les menaces visant l'arrêt du service par l'exploitation d'une faille dans l'implémentation d'un système, processus ou protocole causant un arrêt de processus ou une indisponibilité.

Les menaces relatives au **type 1** sont les suivantes :

- **MD1** : Attaque DoS ou DDoS sur une interface ou plusieurs interfaces (interfaces d'administration ou matérielles).
- **MD2** : Modification des règles d'attribution de bande passante sur les interfaces (interfaces d'administration ou matérielles).
- **MD3** : Modification des règles de partage du canal de communication (protocole de transmission, etc.).
- **MD4** : Modification du routage/isolation des flux d'abonnés permettant à ceux-ci d'accéder illégitimement à des fonctions du socle.
- **MD5** : Modification du routage/isolation des flux d'abonnés permettant à ceux-ci d'accéder illégitimement à des fonctions ou ressources d'un autre abonné ou fonctions tierces.

Les menaces relatives au **type 2** sont les suivantes :

- **MD6** : Modification des configurations des switchs en vue de router du trafic non autorisé sur des interfaces spécifiques et provoquer un (D)DoS. Cette modification peut permettre le détournement des flux.
- **MD7** : Exploitation d'une vulnérabilité protocolaire par une attaque IP (fuzzing, etc.) mettant en cause l'isolation entre VNF.

- **MD8** : Modification de l'image logicielle lors de l'instanciation d'une VNF.
- **MD9 :** Connection sur les comptes d'administration à travers d'une faille logicielle et désactivation ou activation des fonctions sensibles.
- **MD10** : Altération des indicateurs de performance, alarmes, etc. afin de compromettre les processus d'administration.
- **MD11** : Écrasement de mémoire entre VM.
- **MD12** : Modification des ressources matérielles affectées à la VNF par le VIM.
- **MD13** : Modification du processus de configuration des VNF et désactivation des fonctions sensibles.
- **MD14** : Altération, modification ou arrêt d'une ressource matérielle ou virtuelle partagée entrainant l'indisponibilité de la VNF visée par l'attaque.
- **MD15** : Exploitation des capacités d'introspection de l'hyperviseur afin de provoquer un dysfonctionnement de la VNF.
- **MD16** : Quand deux VM appartenant à deux VNF de deux fournisseurs différents cohabitent sur le même nœud de calcul, les ressources (mémoire, processeur, etc.) sont partagées et par conséquence peuvent être attaquées par l'autre VNF grâce à un défaut d'isolation. Une menace sur la disponibilité des données d'une VNF.
- **MD17** : Erreur ou mauvaise gestion des alarmes de congestion par les dispositifs.

9.2.3 Confidentialité

Les menaces affectant la confidentialité des informations relatives aux fonctions sensibles stockées dans les équipements déployés dans le réseau ou transitant sur les interfaces (physiques ou virtuelles) sont divisées en deux types distincts :

1. **Type 1** : Interception de données sensibles pendant leur transit sur le réseau.
2. **Type 2** : Accès aux données relatives aux fonctions sensibles stockées dans le réseau.

Les menaces relatives au **type 1** sont les suivantes :

- **MC1** : Accès aux informations relatives sensibles sur le réseau de l'OCE par un personnel interne malveillant.
- **MC2** : Mise en œuvre d'une duplication de flux, d'un détournement, d'un changement de configuration des VNF.
- **MC3** : Compromission des fonctions d'administration des VNF par un personnel interne malveillant dans le but d'intercepter les flux (déploiement de VNF compromise, modification des configurations de VNF, etc.).
- **MC4** : Compromission de l'hyperviseur et interception des flux sensibles (duplication des flux, déchiffrement des flux).
- **MC5** : Compromission d'une VIM à partir des interfaces d'administration et déploiement de configurations permettant l'interception des données relatives aux

fonctions sensibles (driver compromis, configuration de réseau virtuel, configuration des VNF, etc.).

- **MC6** : implantation d'un dispositif d'écoute sur les interfaces physiques de l'équipement (sondes SFP, etc.).
- **MC7** : installation d'un implant logiciel de duplication des flux sensibles au niveau de l'hyperviseur ou de la VNF.
- **MC8** : instanciation d'une fausse VNF et récupération de trafic.
- **MC9** : plateforme matérielle non authentique réalisant une interception matérielle des flux relatifs aux fonctions sensibles.
- **MC10** : accès aux données sensibles sur les interfaces I/O, la mémoire ou sur les interfaces physiques.
- **MC11** : modification de la configuration réseau à partir d'une VM grâce à un défaut d'isolation et interception des flux sensibles.
- **MC12** : un logiciel malveillant installé dans une VM accède aux interfaces d'une VNF mettant en œuvre des actions illégitimes à travers l'hyperviseur.
- **MC13** : utilisation d'une VNF compromise afin d'intercepter les flux sensibles.
- **MC14** : Compromission de l'hyperviseur et interception des flux sur les interfaces réseaux.
- **MC15** : Compromission des descripteurs de VNF afin d'obtenir un accès privilégié aux fonctions sensibles de la VNF (ajout de comptes, changement des clés d'authentification des comptes d'administration, etc.).
- **MC16** : Compromission du VIM et déclenchement d'une migration d'une fonction mettant en œuvre une action illégitime.
- **MC17** : Modification du routage/isolation des flux d'abonnés permettant à ceux-ci d'accéder illégitimement aux données du socle.
- **MC18** : Modification du routage/isolation des flux d'abonnés permettant à ceux-ci d'accéder illégitimement aux données d'un autre abonné.
- **MC19** : Activation et/ou utilisation d'une fonction non cachée permettant de porter atteinte au secret des correspondances en dehors du cadre légal.

Les menaces relatives au **type 2** sont les suivantes :

- **MC20** : Accès non autorisé aux informations relatives aux fonctions sensibles (cibles, données de configuration, journaux, etc.) à travers un compte d'administration au niveau VNF.
- **MC21** : Accès à la table des fonctions sensibles sur les modules de stockage virtuels ou locaux.

- **MC22** : Accès à l'espace mémoire de la VNF mettant en œuvre des fonctions sensibles et lecture de la table des cibles (à partir de l'hyperviseur).
- **MC23** : Accès à un instantané (snapshot) d'une VNF mettant en œuvre des foncions sensibles et isolation des cibles sensibles dans l'espace mémoire enregistré.
- **MC24** : Compromission des VNF (altération du VNF catalogue, du cycle de vie des VNF, etc.) afin de bénéficier d'un accès privilégié sur une VNF support des fonctions sensibles.
- **MC25** : Accès aux informations relatives aux fonctions sensibles grâce aux capacités d'introspection de l'hyperviseur.
- **MC26** : Quand deux VNF de deux fournisseurs différents cohabitent sur le même nœud de calcul (ou réseau), les ressources (mémoire, processeur, etc.) sont partagées et par conséquent induise une menace sur la confidentialité des données des VNF entre elles (attaque via un défaut d'isolation du nœud).

9.2.4 Intégrité

Les menaces sur l'intégrité des informations sensibles permettant de modifier ces informations stockées dans les équipements réseau ou transitant sur les interfaces (physiques ou virtuelles) sont divisées en deux types distincts :

1. **Type 1** : Modification de données sensibles pendant leur transit sur le réseau
2. **Type 2** : Modification de données sensibles stockées dans le réseau

Les menaces relatives au **type 1** sont les suivantes :

- **MI1** : Compromission de la plateforme matérielle (nœuds de calcul, switch, routeurs, etc.) par un personnel interne malveillant.
- **MI2** : Compromission de l'hyperviseur par un personnel interne malveillant.
- **MI3** : Compromission de l'hyperviseur par un VIM compromis (modification de la configuration ou du binaire de l'hyperviseur, etc.).
- **MI4** : Compromission des VNF (altération du VNF catalogue, du cycle de vie des VNF, etc.) afin de bénéficier d'un accès privilégié sur une VNF support des fonctions sensibles et modification des flux de données sensibles.
- **MI5** : Modification des flux de données sensibles à travers la compromission de l'hyperviseur, nœuds de calcul, VIM, VNF ou le réseau physique (switch, routeurs, etc.)
- **MI6** : Accès privilégié aux comptes d'administrateurs de l'hyperviseur et modification de la configuration réseau en vue de détournement et modification des flux réseau.
- **MI7** : Utilisation malveillante d'un compte administrateur disposant des privilèges susceptibles de compromettre une VNF et manipuler des données sensibles.
- **MI8** : Modification des commandes et données sensibles directement au niveau de l'interface physique de l'équipement grâce à une complicité interne.
- **MI9** : Accès privilégié sur l'hyperviseur ou la VNF et mise en place d'un implant logiciel permettant de modifier les flux de données relatives aux fonctions sensibles.
- **MI10** : Fausse instanciation de VNF et récupération et altération du trafic en transit.

- **MI11** : Attaque directe sur les supports matériels et altération des données stockées (sur le stockage commun, stockage local sur le nœud de calcul, etc.).
- **MI12** : Modification des tables de routage en vue de détournement et modification des flux sensibles.
- **MI13** : Depuis un accès autorisé sur une VNF ou au niveau de l'hyperviseur, accès aux interfaces matérielles et modification des flux sensibles.
- **MI14** : Mise en place d'un détournement du trafic d'une VNF et modification des flux.
- **MI15** : Accès aux interfaces matérielles à partir d'une VNF et modification des flux de données.
- **MI16** : Modification des fichiers de description des VNF, changement des clés ou mots de passe afin de bénéficier d'un accès privilégié sur la VNF en vue d'une compromission des données sensibles.
- **MI17** : Accès à une fonction VNF support de fonctions sensibles depuis un accès privilégié au niveau de l'hyperviseur.
- **MI18** : Modification du routage/isolation des flux d'abonnés en vue de modification de données du socle.
- **MI19** : Modification du routage/isolation des flux d'abonnés en vue de détournement et modification de données d'un autre abonné.
- **MI20** : Modification des fichiers et des éléments liés à la gestion des droits et des rôles
- **M21** : Compromission de VNF d'expositions différentes dans le cas de leurs virtualisations sur un socle commun afin de bénéficier d'un accès privilégié sur une VNF support des fonctions sensibles et modification des flux de données.

Les menaces relatives au **type 2** sont les suivantes :

- **MI22** : Accès et modification non autorisés des informations relatives aux fonctions sensibles du socle (cibles, données de configuration, journaux, etc.) à travers un compte d'administration de l'équipement.
- **MI23** : Altération du scope de réalisation des fonctions sensibles par ajout ou retrait d'éléments dans les systèmes de configuration de ces fonctions (exemple : ajout/retrait de cibles dans la table des interceptions ou déclenchement de code d'une porte dérobée) par l'exploitation d'une faille dans un des processus du système.
- **MI24** : Exploitation d'un compte par défaut ou caché fournissant un accès privilégié.
- **MI25** : Modification des données d'authentification d'un descripteur d'une VNF afin d'accéder aux fonctions sensibles ou décoder les informations chiffrées.
- **MI26** : Accès au contenu de la mémoire de la VNF implémentant des fonctions sensibles à partir de l'hyperviseur ou d'une autre VNF.
- **MI27** : Quand deux VNF de deux fournisseurs différents cohabitent sur le même nœud de calcul (ou réseau), les ressources (mémoire, processeur, etc.) sont partagées et par conséquent induise une menace sur l'intégrité des données des VNF entre elles (attaque via un défaut d'isolation du nœud).

9.2.5 Fonctionnement

Les menaces affectant le bon fonctionnement des fonctions sensibles sont principalement de sept types :

1. **Type 1** : Détournement du trafic véhiculant des données sensibles
2. **Type 2** : Compromission de l'élément de réseau à travers les techniques de virtualisation
3. **Type 3** : Compromission de l'élément de réseau à travers l'environnement d'exécution
4. **Type 4** : Compromission de l'élément de réseau à travers l'administration des fonctions virtuelles (VNF Manager et VIM)
5. **Type 5** : Compromission de l'élément de réseau à travers une interface réseau
6. **Type 6** : Compromission de l'élément de réseau à travers un accès autorisé

Les menaces relatives au **type 1** sont les suivantes :

- **MF1** : Détournement des procédures standards de gestion des fonctions VNF en vue de détourner le trafic sensible vers des fonctions non sensibles (déploiement de fonctions non authentiques, modification des configurations de VM, modification de l'ingénierie réseau interne, etc.).
- **MF2** : Détournement du trafic de données grâce à une attaque utilisant les vulnérabilités des protocoles de routages.
- **MF3** : Détournement du trafic de données grâce à une instanciation de fausse VNF.
- **MF4** : Modification des configurations réseau afin de détourner le trafic des flux de données sensibles.
- **MF5** : Modification du routage/isolation des flux d'abonnés en vue de détournement de données d'un autre abonné.
- **MF6** : Duplication du trafic en utilisant des fonctions disponibles au sein des dispositifs déployés au sein du socle.

Les menaces relatives au **type 2** sont les suivantes :

- **MF7** : Déploiement d'une VNF n'implémentant pas de fonctions sensibles (facturation par exemple) ou non qualifiée par l'OCE sur un nœud opérant des VNF sensibles.
- **MF8** : Accès privilégié aux interfaces d'administration des fonctions sensibles depuis les interfaces physiques d'administration (port console, etc.), ou via les fonctions et interfaces d'administration d'une VNF tierce ou d'un équipement non sensible.
- **MF9** : Accès aux comptes d'administration de la VNF à partir de l'espace de l'hyperviseur.
- **MF10** : Modifications des indicateurs de supervision remontés au VIM afin de déclencher une migration de la fonction réseau sur un hyperviseur compromis.

- **MF11** : Exploitation de faille ou défaut de cloisonnement ou isolation réseau entre les VM et/ou l'hyperviseur afin de prendre le contrôle de la VNF support des fonctions sensibles.
- **MF12** : Exploitation de faille ou défaut de cloisonnement des mécanismes nécessaires à l'application des mises à jour entre les machines virtuelles et l'infrastructure NFV afin de compromettre la NFVI et/ou les VNF.
- **MF13** : Modification des données d'authentification des comptes d'administration d'une VNF afin d'obtenir un accès privilégié.
- **MF14** : Déploiement de VNF non autorisés ou non authentiques permettant de prendre le contrôle de l'élément de réseau ou du réseau interne.
- **MF15** : Compromission de l'hyperviseur à partir d'un code malveillant présent ou introduit sur la VNF.
- **MF16** : Quand deux VNF de deux fournisseurs différents cohabitent sur le même nœud de calcul (ou réseau), les ressources (mémoire, processeur, etc.) sont partagées et par conséquent induise une menace sur le fonctionnement des VNF entre elles (attaque via un défaut d'isolation du nœud).

Les menaces relatives au **type 3** sont les suivantes :

- **MF17** : Attaque offrant un accès privilégié à l'hyperviseur puis compromission de l'hyperviseur dans le but d'altérer les mécanismes d'authentification et de contrôle d'intégrité mis en œuvre dans le déploiement de VNF.
- **MF18** : Modification de la configuration matérielle de l'équipement par les interfaces d'administration de types ILO.
- **MF19** : Modification des KPI afin de déclencher ou de prévenir la migration de la VNF sur un environnement maitrisé par l'attaquant ou d'empêcher la migration de la VNF dans un environnement plus sûr.
- **MF20** : Modification des mécanismes de sécurité mis en œuvre sur la plateforme matérielle par une attaque sur l'interface légitime de configuration Nf-Vi (entre le VIM et l'hyperviseur).
- **MF21** : Attaques permettant un accès aux données de sécurité de l'environnement d'exécution (TPM ou HSM par exemple) afin de compromettre l'authentification matérielle.
- **MF22** : Attaque sur les composants de sécurité matérielle (TPM ou HSM par exemple) mis en œuvre sur l'équipement depuis la machine virtuelle afin de compromettre l'intégrité matérielle.
- **MF23** : Attaque sur l'espace mémoire de la VNF afin d'altérer son fonctionnement.
- **MF24** : Compromission des mécanismes d'authentification et de contrôle d'intégrité mis en œuvre lors des procédures gérant le cycle de vie des machines virtuelles (instanciation, clonage, etc.).

Les menaces relatives au **type 4** sont les suivantes :

- **MF25** : Rebond par le VIM afin de compromettre l'environnement d'exécution, l'hyperviseur ou les VNF (mise à jour du firmware, changement des secrets, changement de configuration, ajout des comptes, etc.).
- **MF26** : Modification de la configuration ou du binaire des fonctions sensibles dans le but de leur désactivation.
- **MF27** : Utilisation d'un code caché dans une VNF afin d'altérer son fonctionnement. C'est un bout de code inutile et résiduel qui peut être manipulé par l'attaquant pour altérer le fonctionnement d'une VNF.

La menace relative aux **types 5 et 6** est la suivante :

- **MF28** : Accès et modification non autorisés aux données de configuration liées à la virtualisation puis reconfiguration des fonctions sensibles.
- **MF29** : Accès à des comptes d'administration privilégiés afin de reconfigurer les fonctions sensibles.

9.2.6 Imputabilité

Les menaces affectant l'imputabilité des actions réalisées par les fonctions sensibles sont divisées en deux types distincts :

1. **Type 1** : La répudiation des actions (modifications des journaux ou des alarmes)
2. **Type 2** : La mobilité des machines virtuelles (furtivité des fonctions virtualisées) liée au cycle de vie (instanciation, migration, etc.)
3. **Type 3** : Activation d'un niveau élevé de journalisation afin de compromettre des informations sensibles ou afin de bloquer par saturation le fonctionnement d'un dispositif.

Les menaces relatives au **type 1** sont les suivantes :

- **MIP1** : Modification des remontées d'alarmes au niveau de la supervision afin de cacher une intervention non autorisée.
- **MIP2** : modification des journaux dans le stockage commun, la mémoire du nœud de calcul, etc.

Les menaces relatives au **type 2** sont les suivantes :

- **MIP3** : Modification des remontées de KPI afin de provoquer ou d'altérer les mécanismes de migration, instanciation de VM et complexifier les possibilités d'analyse d'incidents.
- **MIP4** : Déclenchement de migrations successives afin de complexifier les possibilités d'analyse et d'audit des incidents.

Les menaces relatives au **type 3** sont les suivantes :

- **MIP5** : Activation d'un niveau de journalisation afin de compromettre des informations sensibles. Cette opération peut être accidentelle ou malveillante.
- **MIP6** : Activation d'un niveau de journalisation afin de bloquer par saturation le fonctionnement d'un dispositif. Cette opération peut être accidentelle ou malveillante.

9.2.7 Légitimité et authenticité

Les menaces classées dans cette catégorie affectent la capacité de l'OCE à s'assurer que les composants (fonction réseau, plateforme virtuelle ou matérielle) supportant des fonctions sensibles sont conformes aux caractéristiques de l'équipementier et leurs installations légitimes. A ce titre, les fonctions virtuelles doivent être en mesure d'authentifier la plateforme matérielle sur laquelle elles s'exécutent (y compris la localisation géographique de cette plateforme) et la plateforme matérielle doit s'assurer que l'ensemble de la chaine de démarrage et d'exécution du système est également authentique et intègre.

Les menaces affectant la légitimité des systèmes supports des fonctions sensibles sont divisées en deux types distincts :

1. **Type 1** : Exécution, déploiement de systèmes, composants non authentiques.
2. **Type 2** : Déploiement de systèmes, ou de composants au sein d'environnements d'exécution non authentique.

Les menaces relatives au **type 1** sont les suivantes :

- **ML1** : Déploiement d'un composant non authentique à travers une complicité interne à l'OCE.
- **ML2** : Déploiement d'un composant non authentique à travers d'un accès autorisé sur le système (par ex. à travers le VIM ou d'un accès administration).
- **ML3** : Déploiement de licences logicielles non autorisées par l'OCE.
- **ML4** : Compromission des serveurs de licence.
- **ML5** : Ingérence des équipementiers dans les déploiements des OCEs via un accès au serveur de licence ou via l'obtention d'informations techniques liées aux déploiements des OCEs.
- **ML6** : Installation de systèmes matériels non autorisés au niveau physique (par ex. sonde SFP, etc.).
- **ML7** : Compromission de la procédure d'authentification des VNF.
- **ML8** : Compromission de la séquence de boot afin de permettre l'exécution de logiciels embarqués non authentiques.
- **ML9** : Compromission des données (clés, etc.) utilisées dans la procédure d'authentification des composants authentiques afin de compromettre l'authentification du système.

Les menaces relatives au **type 2** sont les suivantes :

- **ML10** : Compromission des procédures d'authentification des systèmes, logiciels afin de détourner le service de déploiement et instanciation de VNF sur des systèmes non authentiques.
- **ML11** : Accès et modifications des données utilisées dans l'authentification des systèmes matériels (localisation, etc.) afin de contourner la politique de déploiement de l'OCE (relocalisation d'une VNF sur un cloud non autorisé par exemple).
- **ML12** : Changement de la localisation licite d'une VNF vers une autre illicite.

9.2.8 Divers

- **ME1 :** Espionnage industriel entre les fournisseurs des matériels (e.g. nœuds de calcul et de contrôle) au sein du même socle, lors des tests (ou en phase opérationnelles). Cet espionnage pouvant se réaliser par l'accès indu à un ensemble de fichiers de configuration, à des exécutables binaires, des fichiers de logs disponibles sur le nœud ou sur les équipements à proximité. Mais aussi par la mise ou l'activation de sondes pour mesurer le comportement des matériels disponibles sur le même réseau local.
- **ME2 :** Espionnage industriel entre les fournisseurs VNF au sein du même socle. Ces espionnages pouvant se réaliser par l'accès indu à un ensemble de fichiers de configuration, à des exécutables binaires, des fichiers de logs disponibles sur le nœud. Mais aussi par la génération d'erreurs système ou de requête de services mal structurées visant à compromettre le fonctionnement et l'isolation de l'hyperviseur ou du nœud lui-même.
- **ME3 :** Injection depuis un accès utilisateur de trames malformées ou d'avalanche de requêtes à des services du socle pour générer des états instables et propager des erreurs au sein du socle et ainsi sortir le socle de son chemin nominal de fonctionnement.
- **ME4 :** Accès aux outils de tests par un personnel interne malveillant dans le but de compromettre ou contourner le fonctionnement de mises à jour des composants du socle.
- **ME5 :** Accès aux fonctions de mises à jour par un personnel interne malveillant dans le but de compromettre le fonctionnement des composants du socle et l'isolations entre eux.

10 Objectifs de sécurité

Il est proposé un ensemble d'objectifs afin d'améliorer le niveau de sécurité du socle.

Le référentiel propose des objectifs de sécurité qui sont à mettre en œuvre par les OCEs et/ou les fournisseurs.

10.1 Communication

10.1.1 Obj 1 - Communications sécurisées

Les communications doivent protéger les données (flux) dans le plan de contrôle (CP) et le plan usager (UP) en intégrité, en authenticité et, éventuellement, en confidentialité. Les communications concernées sont à minima :

- Entre VNFs.
- VNFM, VIM, Hyperviseur et VNF.
- Nœuds de calcul, Nœuds de contrôle, réseau et stockage commun.

10.2 Stockage et effacement

10.2.1 Obj 2 – Stockage confidentiel et effacement sécurisé des données sensibles

Les données sensibles du socle sont stockées dans trois zones de mémoire qui sont :

1. Stockage commun avec une zone mémoire dédiée et isolée pour chaque VNF,
2. Stockage local des nœuds de calcul
3. Stockage distant sur une solution éventuellement partagée.

Les données sensibles relatives à cet objectif sont celles définies au chapitre 8 'Biens'.

Les données sensibles doivent être

- Protégées en intégrité et en confidentialité préalablement à leur stockage dans les zones de mémoire précitées,
- Effacées de manière sécurisée et définitive lorsqu'elles sont obsolètes.

10.3 Journalisation

10.3.1 Obj 3 – Traçabilité et imputabilité

Les actions et activités au niveau de l'hyperviseur, VIM, VNFM, couche matérielle (Nœuds de calcul et de contrôle, switches, routeurs et stockage commun), VNF et communications entre VNF doivent être traçables. Les journaux collectés sont (liste non exhaustive) : l'identifiant technique de l'entité à l'origine de l'action, l'origine de l'action, la cible de l'action, la date et la nature de l'action, les types des données manipulées, la localisation, les commandes

lancées, un identifiant technique des droits accordés pour procéder à l'action, et les zones mémoires accédées en cours de l'exécution de l'action.

Une sélection de journaux, expurgés des informations sensibles, doit être renvoyée vers le centre des opérations de sécurité (S.O.C.).

Toutes les requêtes venant de l'environnement du socle devront être tracées.

Cet objectif porte aussi sur la gestion des événements de sécurité. Cette gestion doit surveiller les menaces de sécurité en temps réel pour détecter les attaques, les contenir et y répondre. Lorsqu'une attaque est lancée, les données d'analyse sur tous les composants du socle (NFVI, Hyperviseur, VIM, VNFM et VNFs) doivent être fournis.

10.3.2 Obj 4 – Protection des journaux

Les journaux d'évènements générés par les composants du socle doivent être protégés en intégrité, confidentialité et disponibilité. Les journaux/évènements sont horodatés et signés pour en garantir l'authenticité.

Les journaux à protéger sont présentés dans le chapitre 8 'Biens' (Journaux).

Les journaux doivent être protégés lorsqu'ils sont « au repos[7] », pendant leur transmission, leur traitement.

Les journaux ne doivent pas être stockés sur la ressource qui les génère.

Les journaux obsolètes doivent être effacés de manière sécurisée et définitive.

La déclaration d'obsolescence d'un journal doit être soumise à une autorisation de même niveau que l'action la plus sensible contenue dans le journal.

Les habilitations d'accès aux informations de journaux doivent être cohérentes avec les habilitations d'accès aux composants réseaux. Cela ne signifie pas qu'un cloisonnement systématique doive être adopté.

10.4 Contrôle d'accès et clés cryptographiques

10.4.1 Obj 5 – Gestion des identités et des accès

Cet objectif doit couvrir les aspects suivants :

- Les mécanismes de gestion des identités et cycle de vie associés devront être décrits. De plus, le contrôle d'accès mis en œuvre ainsi que la gestion des habilitations (Processus de création, demande, décision d'habilitation) et des secrets d'authentification associés des accédant devront être détaillés.
- Le socle utilise des comptes dits « à privilèges » car permettant des actions d'administration à leurs utilisateurs. La traçabilité des accès privilégiés devra être garantie.

[7] C'est-à-dire lorsque les données résident dans une zone de stockage : fichier / base de données / disque dur / Serveur, etc.

- Authentification des utilisateurs au niveau des différentes couches système. La procédure d'authentification doit être facilement auditable.
- Principe de séparation des rôles et de moindre privilège : l'hyperviseur utilisé doit permettre la gestion de rôles et droits, pour définir des périmètres d'administration et de responsabilités spécifiques à différents administrateurs. Les privilèges accordés aux administrateurs se feront en fonction du juste besoin opérationnel. À titre d'exemple, il n'est pas réalisable que l'administrateur d'une machine virtuelle dispose également des privilèges d'administration du nœud de calcul qui les héberge.
- Il est recommandé de créer des rôles spécifiques à la gestion du stockage et la gestion du réseau.
- Des identités/comptes à fort privilèges ne peuvent être managé par des identités/comptes à plus faibles privilèges. Cette propriété est auditable et contrôlable au niveau de tous les systèmes de management d'un socle.
- Un mécanisme de gestion des privilèges des équipements matériels et logiciels du socle doit être mis en place et cohérent entre ses différents équipements.
- Les équipements matériels et logiciels du socle qui permettent de porter atteinte à des données ou services sensibles doivent mettre en œuvre un cloisonnement des privilèges par l'intermédiaire des rôles.

10.4.2 Obj 6 – Rôles et responsabilités

Tous les rôles donnant un accès (privilégiés ou non) au socle doivent être décrits. Pour chaque rôle, les ségrégations notamment entre les rôles d'administration et les dépendances des droits devront aussi être décrits. Pour chaque rôle, il devra être précisé les commandes autorisées. Les OCEs vérifieront qu'aucune élévation de privilège triviale n'est possible.

Cet objectif permet en particulier de garantir l'authenticité des opérations critiques, c.à.d. pouvant porter atteinte aux biens sensibles (voire chapitre 8) identifiés. Les opérations critiques sont entre autres les suivantes :

- Administration réseau
- Ajout/suppression/Update VNF
- Firmware/SW update
- Gestion des droits d'accès
- Gestion des clés cryptographiques
- Configuration des VIM, VNFM, et VNF
- Configuration des nœuds de calcul et contrôle, Switch, routeur, stockage, etc.

Une cartographie des droits d'administration sur les équipements matériels et logiciels du socle doit être mise en place. La cartographie devra contenir :

- Un schéma Active Directory :
    - Les domaines Active Directory et leur description,
    - Les forêts Active Directory,

- Les relations d'approbation avec les domaines externes à chaque forêt,
- Les caractéristiques des relations d'approbation (bidirectionnelle, filtrée, etc.),
- Les serveurs support des Active Directory ;

- Les infrastructures de gestion de clés ;
- Les systèmes de mots de passe à usage unique ;
- Les systèmes de gestion de journaux et d'évènements de sécurité (collecteurs de journaux, SIEM) ;
- Les systèmes de supervision (alarmes réseau, sondes de détection, etc.).
- La représentation de l'architecture d'administration avec
  - Les zones de responsabilité des différents administrateurs,
  - L'inventaire des secrets (mots de passe, clés, etc.) et droits associés à l'administration des ressources.

Cette cartographie permet, en cas de compromission d'un compte d'administration, d'identifier le niveau de privilège de l'attaquant et la portion du parc potentiellement affectée.

Il est recommandé aux OCEs de respecter les recommandations de l'ANSSI relatives à l'administration sécurisée des systèmes d'information (https://www.ssi.gouv.fr/uploads/2015/02/guide_admin_securisee_si_anssi_pa_022_v2.pdf).

Il est impératif de mettre en place des protocoles sécurisés pour protéger les flux d'administration.

Les opérations d'administration ne doivent jamais être effectuées depuis le réseau public ou depuis un quelconque réseau externe au réseau de l'OCE (un accès VPN étant considéré comme interne).

Toutes les opérations d'administration doivent être journalisées. Ces dernières doivent mettre en œuvre des certificats électroniques propres aux OCEs.

Une campagne d'audit des serveurs d'administration et de tous les composants de la solution d'administration (serveurs, plateforme de rebond, gestion des identités, client d'administration etc.) doit être réalisée tous les 3 ans.

L'administration doit être réalisée sur un réseau logique dédié. L'administration et ou l'exploitation des fonctions sensibles doit être réalisée à minima en utilisant des mécanismes de segmentation logique au sein du réseau d'administration de la zone d'administration sensible. La mise en œuvre d'IPsec, quand elle a lieu, doit respecter les recommandations de l'ANSSI.

10.4.3 Obj 7 – Protection des secrets d'authentification

Les secrets d'authentification présentés dans le chapitre 8 'Biens' doivent être protégés en confidentialité, intégrité et authenticité. Les secrets d'authentification doivent être protégés

lorsqu'ils sont « au repos » et pendant leur transmission et traitement, avec des mécanismes à l'état de l'art des comptes associés audits secrets d'authentification.

Tous les secrets d'authentification anciens et obsolètes doivent être effacés de manière sécurisée et définitive.

10.4.4 Obj 8 – Génération, Gestion, protection et destruction des clés cryptographiques

Les processus et les solutions technologiques assurant une gestion sécurisée des clés cryptographiques doivent être décrits. Ces clés sont utilisées pour le chiffrement au niveau des flux de données sensibles, au niveau des données « au repos » ainsi au niveau des données « en cours d'exécution ».

L'environnement dans lequel est exploité et stocké une clé cryptographique doit être de confiance. Cet environnement doit être sécurisé techniquement et organisationnellement. Les clés stockées sont celles définies au chapitre 8 'Biens' (Clés cryptographiques).

Toutes les clés cryptographiques obsolètes doivent être effacées de manière sécurisée, avec des mécanismes et des niveaux de privilèges cohérents avec la sensibilité desdites clés.

La disponibilité d'une clé doit être garantie pendant tout son cycle de vie.

Les processus de génération, affectation, distribution, négociation, utilisation, renouvellement, recouvrement, et suppression des clés cryptographiques doivent être décrits ainsi que leurs cycles de vie ainsi que le niveau de privilège requis pour procéder à ces opérations.

Une infrastructure de gestion de clés PKI OCE doit être mise en place et dédiée à la gestion de clés cryptographiques et de leurs certificats utilisés au sein du socle. L'autorité de certification doit être de confiance et qualifiée conformément aux normes ANSSI RGS.

10.4.5 Obj 9 – Politique de filtrage

La politique de filtrage doit :

- Protéger le socle contre le fuzzing via des requêtes venant de l'extérieur (Utilisateurs, RAN, interco (roaming), etc.).
- Restreindre les rebonds et contrôler les droits d'accès au socle.
- Rejeter les requêtes malformées ou illégitimes.

Les actions et activités de la politique de filtrage au niveau de l'hyperviseur, VIM, VNFM, couche matérielle (Nœuds de calcul et de contrôle, switches, routeurs et stockage commun) et VNF doivent être traçables dans des journaux. Ces journaux doivent être protégés en intégrité, confidentialité, horodatés et signés pour en garantir l'authenticité.

10.5 Prévention des fuites d'informations

10.5.1 Obj 10 – Prévention des fuites d'informations

Cet objectif porte sur la prévention des fuites d'informations entre :

- VNFs s'exécutant sur des nœuds de calcul séparés. La fuite d'information peut se réaliser à travers un hyperviseur compromis.
- VNFs s'exécutant sur le même nœud de calcul. La fuite d'information peut se réaliser à travers la mémoire et le processeur du nœud de calcul ainsi qu'à travers l'hyperviseur.

10.6 Mutualisation des VNF

Dans cette section on analyse les différents scénarios de mutualisation (matériel, logiciel) et leur impact sur l'isolation au sein du socle.

L'objectif d'isolation est décliné suivant les scénarios de mutualisation décrits en chapitre 5.

10.6.1 Obj 11 – Isolation et Mutualisation de plusieurs VNF au sein du socle

La mutualisation signifie la possibilité d'exécuter deux ou plusieurs VNF sur le même socle. Il y a cinq typologies sur lesquelles l'isolation forte doit être assurée :

- Isolation entre VNF sur un même socle
    - Un socle doit garantir la mise à disposition des ressources requises par une VNF et doit maintenir la disponibilité de ces ressources.
    - Une VNF ne peut altérer les ressources disponibles pour les autres VNF sur un même socle.
    - Une VNF opérationnelle doit explicitement décrire/publier le niveau maximum de ressources requis pour un Traffic maximum préétabli.
    - Toute tentative d'appropriation illégitime, ou non planifiée, non décrite, de ressources additionnelles de la part d'une VNF après son démarrage, doit entrainer son arrêt, la génération des logs précis de ces actions et vue d'une imputabilité de responsabilité sur le fournisseur de la VNF et de potentielles poursuite contractuelles ou légales.
    - Un socle doit garantir les conditions d'usage des VNF dans les gabarits préétablis. Un socle doit interdire tout usage d'une VNF au-dessus des gabarits préétablis.
- Isolation entre VNF et les nœuds de calcul
    - Une VNF ne peut avoir un accès direct à une ressource physique du nœud de calcul.
    - Un nœud de calcul ne doit pas pouvoir détecter ou être informé de la nature des VNF qu'il opère.
- Isolation entre VNF et l'hyperviseur
    - L'hyperviseur doit être prouvé intègre, lors de la phase de boot et cette preuve doit pouvoir être ré-établie à tout instant et de façon aléatoire, de façon à rendre son observation non prédictible.

- L'hyperviseur doit être résistant à :
  - Toute tentative d'instrumentalisation ou détournement des flux internes de mise en relations des VNF avec leurs ressources virtualisées et les entités physiques correspondantes.
  - Toute présence de code ou d'API non renseignées par le fournisseur activable à distance ou directement depuis les VNF.
  - L'hyperviseur doit être dépourvu de fonctionnalités d'inspection du traffic issues ou à destination des VNF, des ressources virtualisées ou physiques.

- Isolation entre VNF et Orchestrateur
  - L'Orchestrateur ne doit à aucun moment avoir un accès direct à une VNF.
- Isolation entre VNF et la plateforme de routage
  - Les flux de données VNF doivent être protégés en intégrité, en authenticité et, éventuellement, en confidentialité.

L'objectif à atteindre est de faire la preuve de chaînage de l'isolation entre ses cinq typologies, en plus de la continuation d'isolation. Cette isolation forte doit être propagée proprement de l'infrastructure virtualisée vers les VNF. Cette isolation de bout en bout doit être auditable, testée, observable et contrôlable via les logs du socle générés.

Le boot sécurisé de l'infrastructure virtualisée pour démarrer les VNF doit être garanti.

Pendant la mise en œuvre et l'exécution de l'infrastructure virtualisée et les VNF, une preuve doit être faite pour garantir la non altération du fonctionnement du socle. Cette preuve doit pouvoir être établie à tout instant et de façon aléatoire, de façon à rendre son observation non prédictible.

L'environnement hébergeant les VNF doit satisfaire les exigences de ses VNF.

Deux VNFs ne pourront être mutualisées que si :

- Elles manipulent des données de sensibilité équivalente (Objectif à court terme). La décision de mutualisation sera prise sur la base d'une analyse de risque,
- Elles manipulent des données de sensibilités différentes (Objectif à moyen terme). La décision de mutualisation sera prise sur la base d'une analyse de risque,
- Elles sont exposées aux mêmes chemins d'attaques (objectif à court terme). La décision de mutualisation sera prise sur la base d'une analyse de risque,
- Elles sont exposées à des chemins d'attaques de nature différente (objectif à moyen terme). La décision de mutualisation sera prise sur la base d'une analyse de risque,
- Elles sont administrées par un même groupe de personne (c.à.d. les mêmes personnes disposent des mêmes privilèges de gestion sur toutes les VNFs mutualisées au sein socle),

  ou

- La solution d'isolation (HW+ SW) mise en place est qualifiée (Objectif à long terme).

Note : Des mécanismes de cloisonnement fiables et vérifiés sont aujourd'hui insuffisante mais susceptible d'évolutions concrètes prochainement.

10.6.2 Obj 12 – Mutualisation du module de sécurité

L'objectif à atteindre est la mutualisation et la centralisation du module de sécurité (e.g. HSM) pour héberger toutes les clés cryptographiques utilisées par le socle.

10.7 Intégrité, Disponibilité et Continuité

10.7.1 Obj 13 - Intégrité d'exécution du socle

Le socle doit garantir que son mode de fonctionnement (intégrité d'exécution, intégrité du code et intégrité des données de configuration) pendant la phase opérationnelle ne peut être modifié que par des personnels autorisés et donc authentifiés.

Le socle doit garantir un démarrage sécurisé de ses composants (secure boot).

Le socle doit interdire l'installation et l'exécution des VNF tierces.

Le socle doit interdire l'altération du VNF catalogue, du cycle de vie des VNF, etc.

Le socle doit garantir l'intégrité et la confidentialité des plans usager et contrôle.

Une VNF doit être insensible au fuzzing (commandes illégitimes, injections des paramètres, tec.) depuis l'utilisateur consommateur du service de la VNF (i.e. flux en provenance de l'Utilisateur). Aucun flux utilisateur ne peut altérer les plans usager et contrôle.

La politique de gestion des utilisateurs ne doit jamais permettre à une personne non autorisée, ni de consulter, ni de modifier tout ou partie de la configuration des composants du socle.

10.7.2 Obj 14 – Disponibilité et restauration du socle

Les équipements matériels et logiciels du socle doivent être disponibles. Le socle doit maintenir en condition de sécurité le VNFM, le VIM, l'hyperviseur et la couche matérielle en temps réel pendant l'opération des VNF.

Le socle doit garantir la mise à disposition des ressources requises par une VNF et doit maintenir la disponibilité de ces ressources.

En cas d'incident, le socle doit pouvoir être restauré. L'objectif vise à rétablir le socle à un point aussi proche que possible du point correspondant au moment de la restauration.

La restauration porte sur les logiciels VNF, VNFM, VIM et hyperviseur ainsi sur le remplacement des équipements (Nœuds de contrôle et de calcul, équipements réseaux et stockages).

Les OCEs doivent mettre en place des mécanismes pour garantir la disponibilité du socle. Les services du socle doivent être réaliser en toute sécurité sans interruption et sans arrêt.

Les OCEs doivent tester le bon fonctionnement des équipements permettant de faire face aux pannes, aux disfonctionnements, aux attaques en déni de service et aux cybers attaques.

Les OCEs doivent tester la résilience de mécanismes, des solutions et des procédures assurant la disponibilité.

Un plan de continuité doit avoir été élaboré afin de traiter les incidents affectant les réseaux.

10.7.3 Obj 15 – Mise à jour et maintenance SW

Cet objectif porte sur les mises à jour de sécurité au niveau logiciels et équipements NFVI, Hyperviseur, VIM, VNFM et VNFs.

Les mises à jour doivent être signées et les rôles qui ont le droit de déployer doivent être listés.

La gestion de mise à jour doit garantir que tous les logiciels et équipements sont à jour des correctifs en vigueur. Les mises à jour doivent être réalisées chaque fois que les fournisseurs des équipements ou logiciels émettent une mise à jour critique. Ces mises à jour peuvent être effectuées par des prestataires externes (mainteneurs, intégrateurs, etc.) exclusivement sous le contrôle de l'OCE.

Le cloisonnement concernant les mécanismes des mises à jour sur les VNFs, le VNFM, le VIM et l'infrastructure NFVI devra s'envisager en tant que de besoin après une analyse des risques.

La gestion des mises à jour doit être fortement cloisonnée vis-à-vis de tous les autres composants du socle au regard des droits très élevés qui sont nécessaires afin d'effectuer les opérations.

Il faut proscrire la mutualisation au sein d'une même zone les fonctions outils de tests et les fonctions de mises à jour.

La maintenance des logiciels doit être possible en maintenant le service du socle.

Tout logiciel qui n'est plus pris en charge par le fournisseur ne doit pas être utilisé, cela signifie que le fournisseur ne fournit aucune mise à jour de sécurité.

Tout logiciel obsolète au sein du socle et ses données doivent être effacés de manière sécurisée et définitive.

Toutes les requêtes concernant les mises à jour des logiciels devront être tracées.

La gestion de mise à jour doit garantir l'atomicité de l'opération : soit une mise à jour complète soit l'annulation de toutes les modifications en cas d'erreur lors du processus.

Il est recommandé de respecter la recommandation de l'ANSSI relative à l'administration sécurisée des systèmes d'information (www.ssi.gouv.fr/securisation-admin-si/) et notamment la recommandation R43 relative à la mise en place de serveurs relais pour la récupération des mises à jour.

La récupération des mises à jour de l'infrastructure matérielle et des machines virtuelles doit être cloisonnée au sein de deux DMZ différentes.

10.7.4 Obj 16 – Maintenance HW

Le remplacement des équipements (Nœuds de contrôle et de calcul) doit être possible en maintenant le service du socle.

10.8 Protection et localisation des données personnelles

10.8.1 Obj 17 – Protection des données personnelles

Les données personnelles des abonnés stockées ou traitées par le socle doivent être protégées en confidentialité.

10.8.2 Obj 18 – localisation des données et fonctions sensibles

Les data centers où les données sensibles sont stockées ou traitées doivent être localisées en France dans le cadre du RGPD.

La localisation des données et fonctions sensibles doit être conforme aux exigences contenues dans la réglementation actuellement applicable au secteur télécom en France.

Cet objectif porte sur la liste (non exhaustive) des données et fonctions sensibles suivantes :

Administration, Sauvegarde, clés cryptographiques, serveurs d'authentification, journaux, etc.

10.8.3 Obj 19 – Sauvegarde

Des sauvegardes régulières doivent être effectuées des données sensibles (clés de chiffrement, serveurs d'authentification, journaux, etc.) afin de pouvoir réagir à une attaque ou un dysfonctionnement du socle. La sauvegarde de ses données est une condition de la continuité du socle.

Les sauvegardes sensibles doivent être protégées en confidentialité et en intégrité. Les sauvegardes sensibles doivent être chiffrées par chaque composant du socle et elles sont transmises ensuite au serveur de sauvegarde.

10.9 Équipements fournisseurs

10.9.1 Obj 20 – Intégration des prérequis fournisseur dans le processus d'achat des équipements

Les processus d'achat des équipements fournisseurs doivent intégrer les prérequis (définis dans le chapitre 6.2 'Prérequis pour les équipements') nécessaires à la mise en œuvre des fonctionnalités de sécurité. Il est nécessaire d'assurer la bonne conformité des équipements fournisseurs aux prérequis définis dans la section 6.2 qui concernent les appels d'offre, les matériels et logiciels.

Cet objectif nécessite des échanges techniques et commerciaux avec les fournisseurs.

10.9.2 Obj 21 – Contrôle de conformité des équipements fournisseurs

Il est nécessaire de contrôler la conformité des équipements fournisseurs à la mise en œuvre (installation, démarrage, activation, etc.) et régulièrement, aux prérequis et exigences intégrer par les OCEs dans le processus d'achat de ces équipements.

Cet objectif nécessite soit des échanges techniques avec les experts produits des fournisseurs, soit des tests opérés directement sur les équipements par les OCEs.

11 Contremesures de sécurité

11.1 Liste non exhaustive des contremesures

Ce chapitre fournit des exemples de contremesures de sécurité concrètes pour répondre aux objectifs cités plus haut dans ce document. Ces contremesures sont les suivantes :

11.1.1 CM1 – Mode 'Build' and 'Run'

Les équipements du socle sont opérés sous deux modes spécifiques : 'BUILD' et 'RUN'.

Le mode 'Build' est le mode actif dans les phases d'intégration et d'implémentation. Il est utilisé avant la mise en production du socle. Le compte root n'est utilisé qu'en mode Build.

Le mode 'RUN' est le mode opérationnel qui est actif dans la phase d'exploitation après la mise en production du socle.

En mode 'RUN', le socle est pleinement opérationnel. Les activités quotidiennes sont réalisées avec des comptes d'exploitation. Sauf pour certaines opérations sensibles et exceptionnelles (par exemple : modification à chaud des équipements, incident, installation d'un correctif d'un patch, etc.), des comptes privilégiés spécifiques sont créés pour pouvoir réaliser ces opérations.

11.1.2 CM2 – Chiffrement de flux

Utilisation de protocoles cryptographiques robustes et à l'état de l'art recommandés par l'ANSSI et mentionnés dans le RGS (par exemple IPsec[8], TLS[9], etc.) pour assurer le chiffrement de flux et tout échange de données et de clés cryptographiques entre les différents composants.

A titre d'exemple :

- L'AES, tel qu'il est spécifié dans le FIPS 197, est un mécanisme de chiffrement symétrique par bloc conforme au référentiel RGS.
- Le mécanisme de chiffrement asymétrique RSAES-OAEP défini dans le document PKCS#1 v2.1 est conforme au référentiel RGS.

11.1.3 CM3 – Chiffrement de stockage

Chiffrement des données sensibles stockées que ce soit en stockage local ou commun (VNF et données VNF stockées dans le stockage local sur les nœuds (de contrôle et de calcul) ou sur le stockage commun du socle, les journaux sensibles stockés, etc.) en utilisant de protocoles cryptographiques robustes recommandés par l'ANSSI conformément au Référentiel général de sécurité (RGS[10]).

[8] https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-ipsec-pour-la-protection-des-flux-reseau/
[9] https://www.ssi.gouv.fr/entreprise/guide/recommandations-de-securite-relatives-a-tls/
[10] https://www.ssi.gouv.fr/guide/cryptographie-les-regles-du-rgs/

A titre d'exemple :

- L'AES, tel qu'il est spécifié dans le FIPS 197, est un mécanisme de chiffrement symétrique par bloc conforme au référentiel RGS.
- Le mécanisme de chiffrement asymétrique RSAES-OAEP défini dans le document PKCS#1 v2.1 est conforme au référentiel RGS.
- Par exemple on peut utiliser :
    - La technologie LUKS en local pour les partitions Linux.
    - La technologie chiffrement CINDER intégré à OpenStack pour les volumes CINDER.

11.1.4 CM4 – Contrôle d'intégrité

Contrôle d'intégrité (ceux-ci peuvent être périodiques, à l'initialisation, aléatoires ou à la demande) du fonctionnement d'une VNF (e.g. vérification de l'intégrité de l'image exécutable d'une VNF, etc.), des données sensibles, clés cryptographiques, journaux, etc. stockées reposant sur une fonction de hachage cryptographique recommandée par l'ANSSI conformément au Référentiel général de sécurité (RGS).

A titre d'exemple, le mécanisme de hachage SHA-256 défini dans le FIPS 180-2 est conforme au référentiel RGS.

11.1.5 CM5 – Effacement sécurisé mémoire

Utilisation d'une solution d'effacement sécurisé des données sensibles, des secrets d'authentification et des clés cryptographiques dans la mémoire dès lors qu'elles ne sont plus utilisées.

A titre d'exemple, une passe d'écriture à zéro de l'ensemble des mémoires ayant contenu des données et clés sensibles constitue un effacement conforme aux règles RGS (Annexe B3 au RGS, section B.1.c.3.1. 'Effacement'.

11.1.6 CM6 – Système de surveillance et de corrélation renforcé

Un système de surveillance et de corrélation centralisé et renforcé qui collecte, remonte et analyse en temps réel des journaux issus des hyperviseurs, VIMs, VNFMs, couche matérielle (Nœuds de calcul et de contrôle, Switches, routeurs et stockage commun), VNF et communications entre VNF.

Ce système permet de :

- Tracer et surveiller les activités sensibles du socle en temps réel.
- Identifier un accès frauduleux au socle ou une utilisation abusive de données et fonctions sensibles (dans le chainage des APIs, etc.) et d'appliquer la politique de réaction adéquate.
- Enregistrer les journaux décrits dans le chapitre 8 'Biens' (Journaux) pour au moins 6 mois.

- Extraire les informations nécessaires en cas d'enquête.

Ce système garantit que les journaux collectés sont authentiques et n'ont pas été altérés. Les journaux sensibles sont stockés et protégés en intégrité, confidentialité, disponibilité et sont horodatées et signées pour en garantir l'authenticité.

Pour les journaux sensibles l'exigence sur la disponibilité est élevée, il est conseillé de mettre en place une réplication de ses journaux.

L'analyse des journaux permet d'assurer que la consommation des ressources dans le socle est normale (fréquence) et correcte. Le système permet également de d'analyser l'ensemble des erreurs système du socle.

Dans le cas d'une anomalie de fonctionnement au sein du socle, le système de surveillance et de corrélation renforcé est capable de déterminer les responsabilités entres les acteurs pour prendre les mesures correctives nécessaires.

11.1.7 CM7 – Système centralisé d'authentification et gestion des droits d'accès

Un système centralisé d'authentification, de gestion des droits et de gestion des habilitations pour :

- Faciliter le contrôle des habilitations et révocations.
- Garantir une authentification adéquate avec le niveau de sensibilité du rôle.
- Limiter le nombre de tentatives d'accès aux comptes utilisateurs sur le socle et bloquer le compte temporairement lorsque la limite est atteinte.
- Imposer un renouvellement des droits d'accès selon une périodicité pertinente et raisonnable.
- Mettre en œuvre des moyens techniques pour faire respecter les règles relatives à l'authentification (par exemple : blocage du compte en cas de non renouvellement du mot de passe).
- Désactiver les comptes par défaut.
- Utiliser des gestionnaires de droits d'accès pour avoir des droits différents pour chaque fonction ou application, tout en ne retenant qu'un mot de passe maître.
- Stocker les secrets d'accès de façon sécurisée (avec au minimum des mots de passe hachés avec une fonction de hachage cryptographique qui utilise un SEL).
- Utiliser un coffre-fort numérique pour stocker les mots de passe des comptes locaux utilisateurs.
- Isoler de bout en bout les flux d'administration.
- Un cloisonnement fort entre les administrateurs par

  - La définition des profils d'habilitation en séparant les tâches et les domaines de responsabilité, afin de limiter l'accès des utilisateurs aux seules données strictement nécessaires à l'accomplissement de leur mission.
  - La création des listes blanches (par exemple les « white List » dans Linux) qui contiennent les commandes autorisées à s'exécuter pour un rôle donné.
- Supprimer les permissions d'accès des utilisateurs dès qu'ils ne sont plus habilités à accéder au socle, ainsi qu'à la fin de leur contrat. Cf. révocation.
- Réaliser une revue périodique des habilitations afin d'identifier et de désactiver les comptes non utilisés et de réaligner les droits accordés sur les fonctions de chaque utilisateur.

Le système d'authentification est conforme aux recommandations RGS de l'ANSSI concernant les mécanismes d'authentification, notamment l'annexe B3[11].

Le système de gestion des droits d'accès est conforme aux recommandations de l'ANSSI parmi lesquelles la sécurisation de l'administration des systèmes d'information[12] et les bonnes pratiques en matière de sécurisation de l'annuaire central Active Directory[13].

Le système de gestion des droits d'accès est conforme aux recommandations de sécurité relatives aux mots de passe[14].

La politique de gestion des droits est gérée de manière extrêmement stricte sous forme RBAC.

Ce système restreint l'accès aux ports de diagnostic et de configuration à distance.

Ce système interdit de manipuler des données sensibles par un mainteneur (tiers ou fournisseur) sans la signature d'un NDA.

Ce système est audité régulièrement.

Pour répondre aux objectifs du cloisonnement des privilèges, les niveaux qu'ils faut définir à minima sur chaque équipement du socle sont les suivants :

- 'Élevé' correspond au niveau le plus privilégié : un compte disposant de ces privilèges pourrait compromettre les VNFs et donc les données sensibles qu'elle manipule.
- 'Moyen' correspond au niveau permettant l'administration de chaque équipement sans offrir les fonctions du niveau 'Élevé' (fonctions permettant de compromettre les VNFs).
- 'Faible' correspond au niveau permettant l'exploitation de chaque équipement sans pouvoir en modifier la configuration.

La stratégie du cloisonnement est la suivante :

[11] https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B3.pdf
[12] https://www.ssi.gouv.fr/entreprise/guide/securiser-ladministration-des-systemes-dinformation/
[13] https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-active-directory/
[14] https://www.ssi.gouv.fr/mots-de-passe.

- Les administrateurs avec un niveau 'Élevé' (disposant des privilèges élevés) réalise uniquement l'installation et la configuration initiale de chaque équipement et les opérations pour lesquels ces privilèges spécifiques sont nécessaires.
- Les administrateurs avec un niveau 'Moyen' réalisent l'administration usuelle de chaque équipement.
- Les utilisateurs avec un niveau 'Faible' réalisent les opérations ne nécessitant aucune modification des composants.

11.1.8 CM8 – Module de sécurité physique pour les clés cryptographiques

Utilisation de module de sécurité de confiance (par exemple un HSM) pour gérer et protéger les clés cryptographiques liées au socle.

L'utilisation, le choix et dimensionnement des mécanismes cryptographiques sont conformes aux règles et recommandations RGS (Annexe B1) de l'ANSSI. Les règles et recommandations contenues dans le guide RGS[15] de l'ANSSI adressent les mécanismes suivants :

- Chiffrement symétrique et asymétrique
- Authentification et intégrité de messages
- Signature
- Authentification d'entités et établissement de clé
- Fonctions de hachage
- Génération d'aléa cryptographique
- Etc.

La gestion des clés est conforme aux règles et recommandations RGS (Annexe B2) de l'ANSSI. Ils adressent le cycle de vie des clés cryptographiques (demande de clé, génération, affectation, introduction, utilisation, fin de vie, renouvellement et recouvrement).

11.1.9 CM9 – Système de filtrage

Un système de filtrage des requêtes peut être mis en place pour analyser et filtrer les flux entrants/sortants sur les composants du socle. Il s'agit de s'assurer que :

- Seules les entités habilitées et/ou autorisées peuvent envoyer des requêtes.
- Aucun client (un tiers externe, un abonné, etc.) ne peut discuter avec le socle.
- Seuls les administrateurs autorisés peuvent accéder au socle.
- Toutes requêtes venant via des interfaces externes doivent être authentifiées, et ne doivent pas perturber le service.

[15] https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0/

- Les accès au socle depuis l'utilisateur à travers les RAN, Internet et interco (roaming data avec les autres OCEs ou interco vers les verticaux), etc. sont contrôlés et surveillés. Les requêtes utilisateur arrivent sur une machine particulière (e.g. UDM en 5G) en entrée du socle et sont filtrées pour ne répondre qu'aux commandes légitimes.

11.1.10 CM10 – Isolation de VNFs au sein du socle

En terme de famille de contremesures, nous avons deux approches pour la mutualisation de ressources pour l'exécution de VNFs :

1. Mutualisation de VNFs de sensibilités identiques, et
2. Mutualisation de VNFs de sensibilités différentes.

Pour les VNF de même sensibilité :

(1) Au niveau des CM (Contremesures) à court terme, une façon à garantir cette isolation au niveau des nœuds de calcul est d'associer à un instant donné un nœud de calcul à une VNF unique (réparation desdites VNF via des clusters de nœuds de calcul). Quand on est sur deux nœuds de calcul séparés, la VNF du nœud X n'est pas capable de compromettre la VNF du nœud Y car elle n'est pas co-localisée. Le nœud X n'est pas capable d'accéder à ou d'altérer la mémoire du nœud Y, ni de compromettre la disponibilité des ressources).

(2) Au niveau des CM à moyen terme, les systèmes décrits dans les CM6, CM7 et CM9 sont capables de détecter des comportements frauduleux ou déviant dans l'exécution des VNF sur un nœud de calcul, depuis l'hyperviseur et d'apporter les mesures correctives nécessaires.

Pour les VNF de sensibilités différentes, des mécanismes de cloisonnement fiables et vérifiés sont aujourd'hui insuffisante mais susceptible d'évolutions concrètes prochainement.

(3) A long terme, l'utilisation des solutions (HW+SW) qualifiées est susceptible de permettre d'obtenir un niveau de confiance suffisant dans la robustesse des mécanismes réalisant le cloisonnement.

11.1.11 CM11 – Isolation entre nœud de calcul et VNF

Les ressources physiques mutualisées du nœud de calcul sont virtualisées au niveau des VNF.

Les utilisateurs du socle qui peuvent accéder au nœud de calcul n'ont pas de droit sur l'utilisation des VNF (par exemple écriture, lecture ou accès au fichier des VNF, actions sur les processus qui sont actifs (arrêter ou relancer un processus), etc.).

Par exemple, les « white list » de linux peuvent être mises en œuvre pour ajouter les commandes autorisées pour les administrateurs du socle qui permettent de faire des tâches non sensibles sur les nœuds sans altérer les VNF.

Les applicatifs et VNF ne peuvent être exécutés sous des privilèges système de type 'root'. Un rôle applicatif spécifique doit être alloué.

Les VNF sont opérées sous deux modes spécifiques : 'BUILD' et 'RUN' comme décrit dans la CM1.

CM10(3) renforce l'isolation entre nœud de calcul et VNF.

11.1.12 CM12 – Isolation entre Hyperviseur et VNF

(1) Un audit et une analyse de sécurité sont conduits par le fournisseur et sont validés par le laboratoire de l'OCE en amont avant la mise en production.

Une procédure de validation est conduite en production. Cette validation consiste à :

- Vérifier le certificat et la signature OCE,
- Vérifier que la version du software est attestée au moment de l'utilisation,
- Vérifier son adressage physique,
- Vérifier la configuration par rapport à un référentiel et assurer que c'est la bonne configuration.

(2) L'hyperviseur est opéré sous deux modes spécifiques : 'BUILD' et 'RUN' comme décrit dans la CM1.

(3) Une contremesure à moyen terme concerne la géolocalisation (exemple : eHealth, les flux doivent rester en France).

(4) Une contremesure à moyen terme est l'utilisation du système de surveillance décrit dans CM6 pour détecter les incohérences comportementales des VNF au niveau de l'hyperviseur.

(5) Une contremesure à long terme est l'utilisation d'un hyperviseur évalué ou certifié. Des nombreux travaux sur la mise en œuvre des schémas d'évaluation et de maintenance adaptés pour ce type de produit sont en cours de réalisation par les autorités de certification nationaux, Eurosmart, Enisa, GSMA, etc.

CM10(3) renforce l'isolation entre hyperviseur et VNF.

11.1.13 CM13 – Isolation entre VNF et Orchestrateur

(1) L'Orchestrateur pilote directement le VNFM et non pas les VNF. Toute communication directe entre l'orchestrateur et un nœud de calcul/VNF est interdite. Un VNFM ne peut pas remonter vers l'orchestrateur.

(2) Un compte Orchestrateur restreint est créé pour accéder au VNFM. Par exemple, les « white list » de linux peuvent être mise en œuvre pour ajouter les commandes autorisées pour l'Orchestrateur qui permettent de faire que des tâches et des opérations prévues.

Des politiques de sécurité sont imposées sur l'Orchestrateur pour une utilisation sécurisée du VNFM.

(3) Un audit par rapport à un référentiel est conduit pour vérifier la configuration de sécurité de l'Orchestrateur.

(4) Le système de filtrage définit dans CM9 peut être utilisé pour identifier les flux de l'Orchestrateur vers le VNFM et les flux entre VNFM et VNF.

(5) Le système de surveillance définit dans CM6 est capable de collecter les logs et d'observer les requêtes et les interfaces Orchestrateur/VNFM, de valider que les règles de sécurité sont

respectées au niveau de l'Orchestrateur et de prendre les mesure adéquates en cas d'anomalies observées.

(6) Une contremesure à moyen terme est de réduire au minimum la surface des API VNFM sensibles.

(7) Une contremesure à long terme est d'utiliser un VNFM générique et non spécifique. L'Orchestrateur se cantonne au fonctionnement normalisé. Un audit et des tests de pénétration peuvent être effectués sur les interfaces VNFM spécifiques.

CM10(3) renforce l'isolation entre orchestrateur et VNF.

11.1.14 CM14 – Isolation entre VNF et routage

(1) Les flux sont chiffrés et authentifiés par IPSec/TLS.

(2) Une contremesure à moyen terme (car elle est soumise à des contraintes de délais, coûts, performance et mise en œuvre) consiste à analyser le comportement d'une VNF pour détecter un comportement inhabituel au niveau routage et réseau (CM6 : Système de surveillance renforcé en temps réel pour analyser les logs et lancer des réactions adéquates).

CM10(3) renforce l'isolation entre routage et VNF.

11.1.15 CM15 – Audit et analyse de sécurité fournisseur

Des audits sont mis en place, des analyses de sécurité sont conduites, les bonnes contremesures sont implémentées et les tests de sécurité sont exécutés avec succès par les fournisseurs des matériels et logiciels.

Les OCEs bâtissent le cadre contractuel avec leurs fournisseurs pour pouvoir transférer de façon directe ou indirecte (via un PASSI ou CESTI) les rapports des audits et d'analyses de sécurité détaillés des tests réalisés, pour atteindre les objectifs du référentiel, sur leurs infrastructures virtualisées.

11.1.16 CM16 – Audit et analyse de sécurité OCE

Des audits et analyses de sécurité sont mis en place régulièrement (tous les 3 ans) par les OCEs que pour les équipements sensibles du socle avec un cycle de maintenance. Ces audits pourront être internes ou réalisés par des prestataires externes labellisés (par exemple PASSI). Le programme de l'audit contient entre autres les éléments suivants :

- Tests fonctionnels,
- Tests de pénétration et tentatives de prise de contrôle,
- Vérification des mesures de sécurité du référentiel,
- Évaluation de la conformité du socle par rapport aux objectifs de sécurité du référentiel.

L'audit et l'analyse de sécurité sont exécutés et partagées avec l'ANSSI préalablement à la mise en service ou à la suite d'une maintenance de sécurité majeure.

11.1.17 CM17 – Utilisation des matériels et logiciels approuvés

L'OCE n'installe que des matériels et logiciels approuvés (sûr et validé) et respecte les guides d'utilisation et de configuration fournis par les fournisseurs. L'intégrité et l'authenticité des logiciels sont à vérifier au chargement, lors du démarrage de l'équipement et pendant l'exécution.

On ne peut pas installer des matériels non approuvés par l'OCE (sécurité technique et organisationnelle). Le socle est protégé par un périmètre physique et toute installation ou ajout d'équipement est donc sous contrôle.

Pour les mises à jour ou installations de logiciels, les contremesures suivantes sont mises en œuvre :

- Opération du socle sous deux modes spécifiques : 'BUILD' et 'RUN' comme décrit dans la CM1.
- Logiciels signés par les OCEs, avec les certificats adéquats et actives/valides à la date d'usage sont utilisables sur un socle.
- Logiciels signés seulement par les constructeurs ou non signés ne peuvent pas s'instancier sur un socle.

11.1.18 CM18 – Système de détection des attaques

(1) A court terme, un SIEM (Security Information and Event Management) est mis en place avec le bon niveau de privilège et d'isolation, de façon à ne pas exposer les objectifs de sécurité. L'objectif de SIEM est de permettre de détecter des attaques grâce à l'exploitation, le filtrage et à la corrélation de logs provenant de différents composants du socle.

(2) Une contremesure à moyen terme est l'extension de SIEM pour détecter des violations d'objectifs de sécurité en temps réel.

11.1.19 CM19 – Boot sécurisé

(1) Le boot de l'hyperviseur est sécurisé avec une vérification de signature. A court terme, un TPM est utilisé sur les nœuds locaux pour sécuriser le boot de l'hyperviseur.

(2) Le boot de l'hyperviseur est assorti d'une preuve d'origine avec une vérification de la localisation (à long terme).

11.1.20 CM20 – Redondance

Des redondances suffisantes sont prévues afin de garantir la continuité de service du socle au niveau de chaque plaque régionale ainsi qu'au niveau national. Cette redondance prend en compte les pannes au niveau transport, au niveau télécom et au niveau énergie.

Il s'agit de deux contremesures pour assurer la haute disponibilité, la continuité et de reprise des activités du socle :

- (1) Court terme : Redondance N+1 : Dans chaque socle, un nœud de contrôle et un nœud de calcul supplémentaires sont disponibles si une attaque DoS est réalisée dans

le but de rendre indisponible les autres nœuds en cours d'exécution. Cette mesure contribue à réduire l'indisponibilité du socle.

- (2) Moyen terme : Architecture géo-redondée : Mise en miroir total du socle dans un environnement distant afin de garantir la récupération complète du socle après un incident.

11.1.21 CM21 – Mise à jour SW

Les mesures pour assurer la mise à jour et la maintenance correctes et sécurisées des logiciels au sein du socle sont entre autres les suivantes :

- Opération du socle sous deux modes spécifiques : 'BUILD' et 'RUN' comme décrit dans la CM1.
- Mises à jour et maintenance des VIM, VNFM et VNF par les mainteneurs (fournisseurs ou tiers).
- Mise à jour de l'hyperviseur par l'OCE. Cette mise à jour peut être déléguée à un mainteneur (fournisseurs ou tiers).
- Suivi régulier des mises à jour.
- Vérification régulière que la dernière version du logiciel est installée et exécutée.
- La mise à jour des briques logiciels du socle est toujours validée préalablement sur un environnement de test ou de pré-production.
- Les logiciels du socle ne sont pas exposés sur Internet. Pour récupérer les mises à jour sur Internet, une machine séparée est utilisée. Ces mises à jour ensuite sont copiées vers un serveur web local ou sur un disque amovible (clé USB, CD- ROM). La machine qui effectue le téléchargement des mises à jour sur Internet, est protégée par un pare-feu. Ce dernier est configuré pour n'autoriser que les flux depuis cette machine vers les adresses IP des services de mises à jour officiels sur les ports associés. Une fois le téléchargement des mises à jour est terminé, la machine est désactivée.
- Aucun accès direct depuis ou vers internet.
- Mises à jour et maintenance des VIM, VNFM et VNF par les mainteneurs (fournisseurs ou tiers). Le mainteneur vérifie si la mise à jour a été effectuée avec succès dans son intégralité.
- Mise à jour de l'hyperviseur par l'OCE. Cette mise à jour peut être déléguée à un mainteneur (fournisseurs ou tiers). L'OCE ou mainteneur vérifie si la mise à jour a été effectuée avec succès dans son intégralité.
- Le service de mise à jour des VNFs est cloisonné vis-à-vis de ceux de l'infrastructure NFV, VIM et VNFM. Plusieurs machines différentes sont utilisées pour télécharger les mises à jour.

11.1.22 CM22 –Conformité au RGPD

La conformité au RGDP des OCEs et la localisation en France des data centers garantissent la confidentialité des données personnelles et un traitement de ces données respectant la vie privée.

11.1.23 CM23 - Sauvegarde

La protection en confidentialité des sauvegardes est effectuée par chaque composant du socle. Les sauvegardes sont chiffrées par chaque composant et elles sont transmises au serveur de sauvegarde. Les clés de chiffrement ne sont jamais transmises au serveur de sauvegarde. Les clés de chiffrement de chaque sauvegarde ne sont jamais contenues dans les sauvegardes. Les données contenues au niveau du serveur de sauvegarde ne permettent pas l'accès aux données sauvegardées.

11.2 Tableau de classification des contremesures

Ce tableau classifie les contremesures selon leur état actuel de la mise en œuvre. Les contremesures sont divisées en trois catégories : disponible, en cours d'implémentation, future (pas encore en œuvre).

Contremesures	Disponible	Court terme	Moyen terme	Long terme
CM1	X			
CM2	X			
CM3	X			
CM4		X		
CM5	X			
CM6			X	
CM7		X		
CM8		X		
CM9			X	
CM10 (1)		X		
CM10 (2)			X	
CM10 (3)				X
CM11	X			
CM12 (1)		X		
CM12 (2)	X			
CM12 (3)			X	

CM12 (4)			x	
CM12 (5)				x
CM13 (1)	x			
CM13 (2)		x		
CM13 (3)		x		
CM13 (4)			x	
CM13 (5)			x	
CM13 (6)			x	
CM13 (7)				x
CM14 (1)	x			
CM14 (2)			x	
CM15				x
CM16				x
CM17			x	
CM18 (1)		x		
CM18 (2)			x	
CM19 (1)		x		
CM19 (2)				x
CM20 (1)		x		
CM20 (2)			x	
CM21		x		
CM22		x		
CM23	x			

Table 3 Classification des contremesures

12 Synthèses de correspondance

12.1 Synthèse des protections contre les menaces identifiées

Le tableau suivant présente la couverture des menaces par les objectifs de sécurité :

Objectifs de sécurité	Menaces associées
Obj 1	Confidentialité : Menaces Type 1, Intégrité : Menaces Type 1
Obj 2	Confidentialité : Menaces Type 2, Intégrité : Menaces Type 2
Obj 3	Imputabilité : Menaces Types 1, 2 et 3
Obj 4	Confidentialité : Menaces Types 1 et 2, Intégrité : Menaces Types 1 et 2, Disponibilité : Menaces Types 1 et 2
Obj 5	Légitimité et authenticité : Menaces Types 1 et 2
Obj 6	Légitimité et authenticité : Menaces Types 1 et 2
Obj 7	Confidentialité : Menaces Types 1 et 2, Intégrité : Menaces Types 1 et 2, Disponibilité : Menaces Types 1 et 2
Obj 8	ME3, Fonctionnement : Menaces Types 1, 2, 3, 4, 5 et 6
Obj 9	ME3, Disponibilité : Menaces Types 1 et 2, Fonctionnement : Menaces Types 1, 2, 3, 4, 5 et 6
Obj 10	ME1, ME2, Confidentialité : Menaces Types 1 et 2
Obj 11	Toutes les Menaces sont applicables
Obj 12	ME3, Disponibilité : Menaces Types 1 et 2, Fonctionnement : Menaces Types 1, 2, 3, 4, 5 et 6
Obj 13	Intégrité : Menaces Types 1 et 2
Obj 14	Disponibilité : Menaces Types 1 et 2
Obj 15	ME3, ME4, ME5, Fonctionnement : Menaces Types 1, 2, 3, 4, 5 et 6
Obj 16	ME3, ME4, ME5, Fonctionnement : Menaces Types 1, 2, 3, 4, 5 et 6

Obj 17	Confidentialité : Menaces Types 1 et 2, Intégrité : Menaces Types 1 et 2
Obj 18	Légitimité et authenticité : Menaces Types 1 et 2
Obj 19	Disponibilité : Menaces Types 1 et 2
Obj 20	Toutes les Menaces sont applicables
Obj 21	Toutes les Menaces sont applicables

Table 4 Couverture Objectifs - Menaces

12.2 Matrice de correspondance Objectifs-Contremesures

La matrice suivante met en correspondance les objectifs et les contremesures à implémenter pour réponde à ses objectifs.

Objectifs de sécurité	Contremesures																						
	CM1	CM2	CM3	CM4	CM5	CM6	CM7	CM8	CM9	CM10	CM11	CM12	CM13	CM14	CM15	CM16	CM17	CM18	CM19	CM20	CM21	CM22	CM23
Obj 1		X							X									X					
Obj 2			X	X	X													X					
Obj 3						X	X		X									X					
Obj 4			X	X	X													X					
Obj 5							X											X					
Obj 6							X		X									X					
Obj 7							X											X					
Obj 8					X		X	X										X					
Obj 9						X			X									X					
Obj 10	X	X	X			X				X	X	X	X	X				X					
Obj 11	X	X	X	X		X				X	X	X	X	X			X	X	X		X		
Obj 12		X	X					X										X					
Obj 13	X			X		X			X	X	X	X	X	X			X	X	X				
Obj 14	X			X		X												X		X			

Obj 15	X																X	X			X		
Obj 16	X																			X			
Obj 17		X	X															X				X	
Obj 18																		X				X	
Obj 19																							X
Obj 20															X	X							
Obj 21															X	X							

Table 5 Couverture Objectifs - Contremesures