Retour d'expérience sécurité sur le déploiement des technologies SDN/NFV

Jean-Michel Farin and Grégory Veille

Orange France {jean-michel.farin,gregory.veille}@orange.com

Abstract. Les technologies SDN/NFV sont amenées à être de plus en plus utilisées par les opérateurs de communications électroniques pour répondre rapidement aux besoins du marché et particulièrement pour le déploiement du réseau mobile 5G. Orange France propose ici un retour d'expérience sur la mise en place de ces technologies d'un point de vue sécurité. Il y est décrit la problématique principale liée au fait d'exécuter une fonction réseau sur une infrastructure non maîtrisée. Pour comprendre ce problème, les différents éléments constitutifs d'une infrastructure de virtualisation pour des fonctions réseaux sont détaillés avec leurs différentes faiblesses pour une utilisation dans ce contexte. La sécurité des équipements réseau physiques et leurs équivalents virtualisés sont ensuite comparés et quelques éléments périphériques et mesures de sécurité pour atténuer les risques sont présentés. Enfin la question du rôle important de la supervision de sécurité est abordée.

Keywords: SDN · NFV · Telco Cloud · infrastructure · disponibilité · confidentialité · supervision

1 Introduction

Les technologies SDN/NFV sont amenées à être de plus en plus utilisées par les opérateurs de communications électroniques pour répondre rapidement aux besoins du marché et particulièrement pour le déploiement du réseau mobile 5G.

En effet, ces technologies permettent la virtualisation des fonctions réseaux nécessaire à l'arrivée de l'automatisation du déploiement de services réseaux. Mais, pour s'exécuter, ces fonctions réseaux virtualisées ont besoin d'un socle : l'infrastructure de virtualisation. Cette infrastructure de virtualisation étant répartie au niveau géographique sur plusieurs sites des opérateurs, contrairement à un Cloud centralisé, et dédiée à l'exécution de fonctions réseaux, on parle dans notre cas de "Telco Cloud".

Techniquement parlant, ce "Telco Cloud" reprend les éléments d'infrastructure d'un Cloud classique avec, toutefois, quelques optimisations pour la gestion de paquets IP. Ce "Telco Cloud" peut être fourni par un équipementier sur lequel il exécute ses fonctions réseaux virtualisées, par un sous-traitant spécialisé dans la gestion d'infrastructure de virtualisation, par l'opérateur lui-même voire par un acteur du Cloud classique en mode "Network as a Service". Dans le cas d'Orange France, c'est la solution où l'opérateur

gère lui-même son “Telco Cloud” qui a été retenue et Orange joue donc le rôle d'intégrateur d'infrastructure de virtualisation. Les conclusions qui ont été tirées sont toutefois également valides pour les autres cas même si alors la répartition des responsabilités est différente.

2 Le besoin d'une infrastructure de virtualisation de confiance

En tant qu'opérateur de communications électroniques, Orange France propose des services de transmission d'informations à distance grâce à des fonctions réseaux fournies par des équipements spécialisés. Ces fonctions réseaux sont diverses : routage IP/MPLS, réseau d'accès (fixe ou mobile), cœur de réseau mobile, gestion de la voix sur IP, etc. Chacune joue un rôle précis et nécessite des compétences particulières pour être administrée.

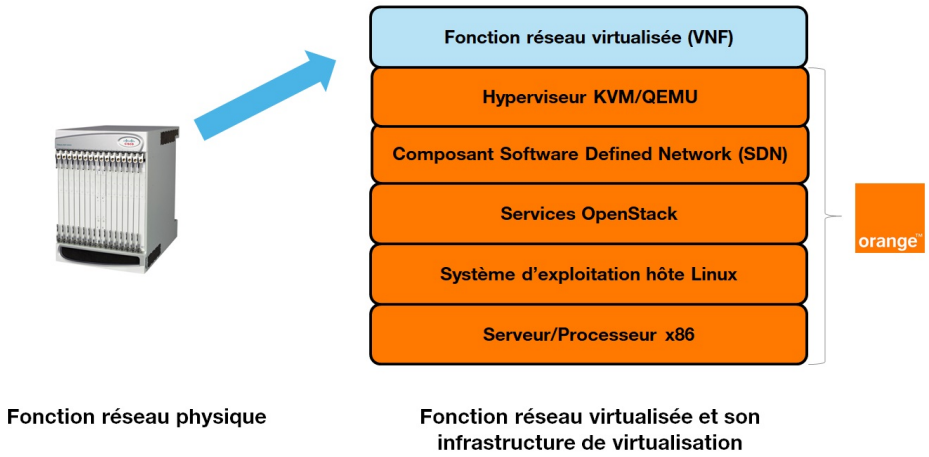
Ces équipements font partie des actifs les plus sensibles de l'entreprise car le service rendu aux clients est dépendant de leur bon fonctionnement. De plus, l'opérateur de communications électroniques est soumis à un cadre réglementaire important - continuant à se renforcer pour la 5G [1] - ayant un impact sur le choix et la configuration des équipements. Ainsi, certains équipements ont des besoins en disponibilité plus importants, comme par exemple ceux utilisés en cœur de réseau, et d'autres manipulent des données sensibles soumises à la réglementation nécessitant un haut niveau de confidentialité, comme par exemple pour respecter le règlement général sur la protection des données (RGPD) ou le secret de la correspondance. Ces contraintes s'appliquent indifféremment aux fonctions réseaux physiques ou virtualisées. Cependant, dans le cadre de la virtualisation, elles s'étendent à l'infrastructure de virtualisation support de ces fonctions.

Au niveau de l'infrastructure de virtualisation, ces contraintes s'ajoutent aux nouvelles contraintes propres à la virtualisation en elle-même. Il faut en effet prendre en compte que les infrastructures de virtualisation sont constituées de différentes briques ayant chacune des problématiques techniques et de sécurité particulières. De plus, les compétences humaines requises pour la gestion d'un Cloud ne sont pas les mêmes que celles jusque-là demandées au personnel en charge des réseaux. Et comme le “Telco Cloud” a vocation à être mutualisé pour y exécuter des fonctions réseaux diverses, son exploitation a été confiée par Orange France à une équipe spécialisée et non aux équipes déjà en charge de l'exploitation des fonctions réseaux. Cela rend d'autant plus complexe la mise en place de mesures pour garantir disponibilité et confidentialité.

La sécurisation des fonctions réseaux en tant que telle n'étant pas liée à la virtualisation, cet article se concentre sur la sécurisation de l'infrastructure de virtualisation.

3 Eléments constitutifs d'une infrastructure de virtualisation pour des fonctions réseaux

Différentes solutions existent sur le marché pour constituer une infrastructure de virtualisation. Dans le cas des premiers déploiements d'Orange France, le choix s'est porté vers une infrastructure constituée de matériel x86, d'un système d'exploitation Linux, de services OpenStack, d'une solution SDN (Software Defined Network) et de l'hyperviseur KVM. Nous ne reviendrons pas dans cet article sur les raisons des choix de ces composants. Les conclusions sont valables pour d'autres solutions car les faiblesses des différents composants peuvent être considérées comme équivalentes ou proches.



3.1 Le matériel

Le premier élément de la chaîne est le matériel c'est-à-dire le serveur x86. Les serveurs sont répartis en plusieurs catégories : serveurs de stockage, serveurs de calcul, serveurs de contrôle. En fonction de leurs rôles, leurs caractéristiques sont adaptées. Ainsi, le serveur de stockage disposera de capacité en espace disque important et le serveur de calcul fonctionnera avec des processeurs plus rapides. Les fonctions réseaux seront exécutées réellement sur les serveurs de calcul mais leurs disques durs virtuels seront déportés sur les serveurs de stockage. Les serveurs de contrôle serviront eux à orchestrer les autres.

Dans tous les cas, ces serveurs nécessitent une analyse de sécurité particulière. En effet, plusieurs failles dans les processeurs Intel [2] ont été dévoilées récemment et ont un impact sur la sécurité de la virtualisation. De même, plusieurs études sur les cartes de gestion "BMC" tels HP iLo [3], Dell iDRAC [4], IBM IMM,etc. ont montré qu'elles pouvaient constituer un vecteur d'attaque et devaient, par conséquent, faire l'objet d'une attention particulière. Il est également important de noter que divers microprogrammes sont installés sur le matériel (carte BMC, BIOS, carte réseau, carte RAID, etc.) et une gestion

des vulnérabilités de ces microprogrammes doit être mise en place et incluse dans le processus de mise à jour des versions.

3.2 Le système d'exploitation

Le deuxième élément de la chaîne est le système d'exploitation Linux. Le système d'exploitation va servir à exécuter les applications nécessaires à la virtualisation sur le matériel physique. Afin d'homogénéiser le déploiement et, par conséquent, faciliter le travail de mise à jour de sécurité, Orange a fait le choix d'utiliser le même système d'exploitation sur les différents types de serveurs.

Le système d'exploitation est constitué de nombreux logiciels et bibliothèques et d'un noyau intégrant de nombreux modules pour répondre à des besoins hétérogènes. Etant donné son rôle central, il doit faire l'objet d'une sécurisation renforcée pour ne pas mettre en danger les fonctions réseaux virtualisées hébergées. Une gestion des vulnérabilités de ce système d'exploitation et des logiciels embarqués doit ici aussi être mise en place. Le processus de mise à jour des versions doit également être mis en place et en lien avec le matériel utilisé. En effet, une mise à jour d'un microprogramme du matériel peut nécessiter une mise à jour du noyau ou d'un pilote au niveau du système d'exploitation. De même, une faille dans le processeur peut nécessiter également une mise à jour du noyau du système d'exploitation.

3.3 Les services OpenStack

Le troisième élément de la chaîne est OpenStack. OpenStack est un ensemble de logiciels permettant la gestion de ressources matérielles pour les partager entre plusieurs machines virtuelles. C'est grâce à cet ensemble de logiciels que, via des API dites "externes", Orange peut instancier la création d'une fonction réseau virtuelle qui sera exécutée dans plusieurs machines virtuelles réparties sur des serveurs de calculs différents avec des disques virtuels hébergés sur les serveurs de stockage. Ce sont ces logiciels qui permettent de gérer les composants matériels en mode "Cloud" c'est-à-dire "à la demande".

Ces logiciels interagissent également via des API cette fois dites "internes". Au niveau de la sécurité d'OpenStack, plusieurs éléments posent problème : aucune matrice de flux entre les logiciels n'est disponible, les mots de passe d'administration se retrouvent en clair dans des fichiers de configuration, les flux entre les services ne sont pas sécurisés, les disques virtuels des machines virtuelles ne sont pas chiffrés, etc. Dans le cas d'un "Telco Cloud" distribué géographiquement dans des salles réseaux et exécutant des fonctions contenant des données sensibles, cela n'est pas acceptable et un travail de sécurisation d'OpenStack doit avoir lieu. Orange France a par conséquent mis en place de nombreux mécanismes de sécurisation à ce niveau en se basant sur le guide de sécurité OpenStack [5]. Mais, même avec ce travail de sécurisation, le nombre de services installés et la non maîtrise globale du système par une entité donnée laisse perplexe sur la sécurité de l'ensemble. Il convient par conséquent de mettre

en place des mesures organisationnelles et de supervision spécifiques dont nous parlerons plus loin dans ce document.

3.4 Le composant SDN

Le quatrième élément de la chaîne est le composant SDN (Software Defined Network). Le SDN est constitué d'un contrôleur et de routeurs virtuels déployés sur les serveurs de calcul. Il permet le routage des flux entre les différentes fonctions réseaux virtualisées et le réseau réel. Ainsi, c'est grâce à ce composant que les flux réseaux sont envoyés par le routeur vers le bon serveur de calcul exécutant la machine virtuelle de la fonction réseau virtualisée cible. Cela permet une gestion dynamique des flux nécessaire au fonctionnement en mode "Cloud" des fonctions réseaux virtualisées qui peuvent ainsi s'adapter au trafic reçu à un instant t en modifiant le nombre de serveurs de calculs utilisés.

En dehors des questions de sécurisation de son administration qui sont les mêmes que pour tout autre élément, ici le principal problème rencontré par Orange France est l'impact qu'il peut avoir sur les mises à jour des autres composants. En effet, la partie routeur viruel du SDN a des interactions fortes avec les cartes réseaux et le système d'exploitation et la partie contrôleur SDN avec OpenStack. Toute mise à jour d'un de ces composants peut par conséquent avoir un impact sur les performances voir la stabilité du SDN. Et inversement, toute mise à jour du SDN peut nécessiter une mise à jour d'un autre composant qui n'était pas planifié. Ce composant doit donc bien être pris en compte dans le processus de gestion des mises à jour et faire l'objet d'une sécurisation renforcée.

3.5 L'hyperviseur

Le dernier élément de la chaîne est l'hyperviseur KVM. L'hyperviseur est le logiciel qui va permettre l'exécution de machines virtuelles sur une machine physique. Ces machines virtuelles sont utilisées par les fonctions réseaux virtuelles pour s'exécuter.

KVM, Kernel Virtual Machine, est un hyperviseur constitué d'un composant intégré au noyau Linux et d'un composant dans l'espace utilisateur intégré à QEMU. Ce composant est lui aussi critique car il doit garantir la stabilité des fonctions réseaux et leur cloisonnement. Or, comme pour les composants pécédents, celui-ci doit savoir répondre à des besoins hétérogènes dans des environnements hétérogènes. Dans ces conditions, l'analyse de sécurité doit porter sur l'organisation mise en place par les développeurs pour gérer les interactions entre les nouvelles fonctions qu'ils développent, ou les mises à jour des fonctions existantes, et les effets sur un contexte d'utilisation donné. La consultation des bugs trackers de KVM [6] et QEMU [7] montre que les bugs ne sont pas forcément corrigés et malheureusement la disponibilité des informations pour reproduire ceux-ci pourrait aider des personnes malintentionnées à mettre en œuvre des attaques.

4 Comparaison entre un équipement réseau physique et un équipement virtualisé

La sécurisation des équipements réseaux physiques est le résultat de longues années de travail commun entre les opérateurs et les équipementiers. Aujourd'hui, beaucoup de risques sont traités et les réseaux peuvent être considérés comme fiables. Avec l'arrivée des équipements virtuels, de nouveaux acteurs entrent en jeu comme nous l'avons vu dans la partie précédente et ces acteurs ne fournissent pas de solutions dédiées pour être utilisées par des opérateurs de communications électroniques.

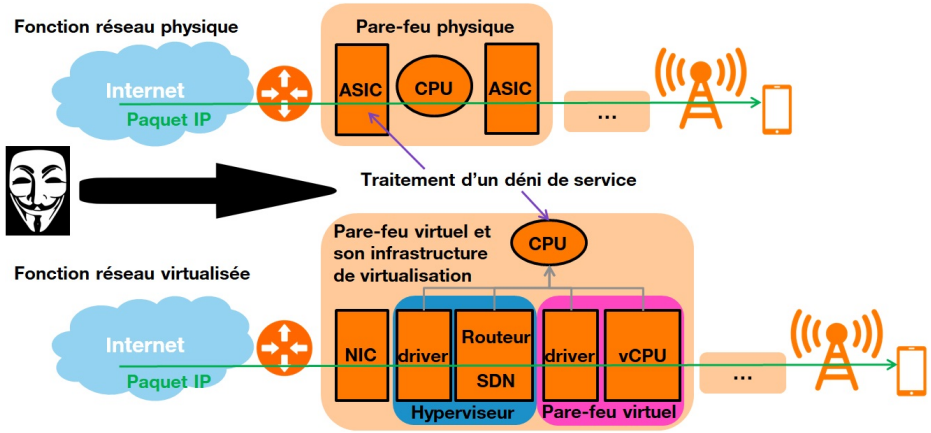
La première difficulté vient de la différence de conception physique des équipements. En effet, les équipements réseaux physiques sont dans la majorité des cas composés de différentes cartes de traitement divisées en deux familles : les cartes traitant le plan de données, également appelé plan utilisateur, et les cartes traitant le plan de contrôle. Les paquets IP en transit sur l'équipement sont traités par les cartes dédiées au plan de données. Les paquets IP à destination de l'équipement lui-même ou pour lesquels les cartes du plan de données ont besoin d'une analyse sont traités par les cartes dédiées au plan de contrôle. Ces différentes familles de cartes sont équipées de processeurs, ASIC ou FPGA choisis par l'équipementier pour leur efficacité dans le traitement des tâches à effectuer par celles-ci. Pour un opérateur comme Orange, cette distinction permet de mettre en place des mesures de protection contre des attaques sur les cartes disposant du matériel le plus adapté au traitement demandé. Ainsi, le plan de contrôle d'un équipement peut être protégé contre les accès illégitimes via la mise en place de filtres de paquets IP sur les cartes du plan de données plus performant dans ce type de traitement. Des mécanismes de limitations de bande passante peuvent aussi être mis en place sur ces cartes pour protéger l'équipement d'attaques de type déni de service distribué pour les mêmes raisons.

Dans le cas de la virtualisation, en l'état actuel des choses, il n'y a pas de cartes physiques sur lesquelles des protections peuvent être mises en place. Les paquets IP passent forcément par la carte réseau du serveur de calcul, puis par le pilote du système d'exploitation hôte, puis par le routeur virtuel SDN, puis, via l'hyperviseur, il est transmis à la machine virtuelle dans laquelle il est traité par le pilote du système d'exploitation de celle-ci pour enfin être traité par la fonction réseau. Le passage par toutes ces étapes augmente les risques de déni de service via, par exemple:

- un paquet malformé posant problème à un des composants traversés,
- un accès illégitime au plan de contrôle qui ne serait pas protégé,
- une consommation excessive de ressources processeur lors du traitement à chaque étape de la chaîne de paquets d'une attaque de type déni de service distribuée.

Dans l'exemple ci-dessous, une attaque de type déni de service est arrêtée sur un pare-feu physique positionné entre Internet et les abonnés mobiles Orange au niveau de l'ASIC de la carte réseau support de l'interface d'entrée du paquet IP. Par contre, dans le cas de la virtualisation, ce sera à un des composants logiciels de détecter l'attaque et de la faire traiter par le CPU du serveur de calcul. On

voit qu'il y a un risque de saturation du CPU qui doit traiter plusieurs fois le même paquet IP malveillant à chaque passage d'un composant logiciel.



Le fait d'utiliser de multiples fournisseurs ne permet également pas de bénéficier aujourd'hui de contrôle d'intégrité des serveurs de calcul comme c'était le cas avec des équipements physiques. En effet, dans le cas de l'équipement physique, l'équipementier maîtrise le matériel, le chargeur de démarrage et le système d'exploitation. Il a donc la maîtrise totale de l'environnement technique pour mettre en place des contrôles d'intégrité sur les microprogrammes, systèmes d'exploitation et applications installés. Dans le cas de la virtualisation, il faut déployer une solution permettant de vérifier tous les composants des différents acteurs et cette solution doit être interrogeable par les orchestrateurs de fonctions réseaux virtuelles pour savoir si ils peuvent ou non déployer une fonction sur un serveur de calcul donné et vérifier qu'elle a été correctement déployée avant de lui envoyer du trafic. A défaut d'avoir cette solution globale de démarrage sécurisé avec attestation à distance, Orange a décidé de se limiter, dans un premier temps, à vérifier au mieux l'intégrité de chaque composant avec une solution dédiée à chaque étape. Cela demande un travail conséquent d'intégration et d'exploitation par rapport à l'utilisation d'une solution déjà prête fournie par l'équipementier de la fonction réseau physique.

Au niveau de la gestion des habilitations des exploitants, les équipementiers mettent à disposition sur leurs équipements des mécanismes permettant de gérer les commandes autorisées aux exploitants en fonction de profils ou rôles via des Role-Based Access Controls (RBAC) et/ou la possibilité de déporter les vérifications de droits d'exécution des commandes à des services de type AAA (Authentification, Authorization, Accounting) comme par exemple TACACS+. Cela permet de maîtriser les droits donnés aux différentes équipes d'exploitation et même d'interdire certaines commandes qui peuvent se montrer dangereuses en environnement de production. De plus, les commandes tapées sont journalisées. En tant qu'opérateur, Orange attend de l'infrastructure de virtualisation le même type de fonctionnalité mais, ici aussi, du fait de l'utilisation de différents composants "génériques", la tâche n'est pas simple. Il faut ainsi par exemple pour

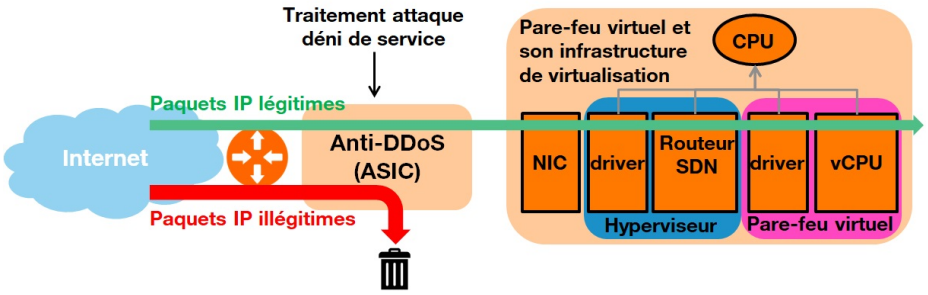
le système d'exploitation Linux utiliser des comptes nominatifs associés à des groupes ayant des autorisations d'élévation de privilèges particulières.

Enfin, les processus de gestion des fournisseurs sont largement complexifiés. Pour assurer la sécurité du réseau, l'opérateur se doit de s'assurer que ses fournisseurs prennent des engagements sur la sécurité et suivent de bonnes pratiques de sécurité dans le développement de leurs produits et leur suivi. Le respect de ces engagements et du suivi des bonnes pratiques fait l'objet de contrôles de la part de l'opérateur. Dans le cas de la virtualisation, le nombre de fournisseurs augmentant et les limites des domaines de responsabilité pouvant ne pas être clairs, le risque de défaut est plus important et le travail de vérification peut être trop important pour être totalement mené à bien.

5 Eléments périphériques et mesures de sécurité

Comme nous l'avons vu, les composants choisis pour la mise en place du "Telco Cloud" Orange France ne permettent pas d'atteindre à elles seules un niveau de sécurité approchant celui dont Orange disposait avec du matériel dédié. Pour diminuer les risques, des éléments périphériques et des mesures spécifiques de sécurité doivent être mises en place.

Pour se prémunir des attaques de type déni de services, en attendant des solutions de type "carte réseau intelligente" (SmartNIC), Orange a mis en place des protections sur des équipements physiques en amont de l'infrastructure de virtualisation. Cependant, même si cela a du sens dans le cas d'une infrastructure de virtualisation de type "IT Cloud" déployée en centre de données, pour un "Telco Cloud" distribué géographiquement cela ne peut être qu'une mesure transitoire.



Il est de plus indispensable de mettre en place une solution de gestion des accès de type AAA (Authentification, Authorization, Accounting) offrant des services de gestion de l'identité et des droits des exploitants sur les composants du "Telco Cloud". Cette solution devra pouvoir être utilisée par les composants matériels, le système d'exploitation Linux, les services OpenStack et le service SDN, et même à terme par les VNF et leurs gestionnaires. Cette solution devra être couplée à des mesures organisationnelles pour permettre la protection des données traitées par les fonctions réseaux de menaces provenant de la mise à disposition de droits étendus sur l'infrastructure de virtualisation. Ainsi, un

exploitant de l'infrastructure de virtualisation ne devra pas pouvoir disposer des droits de type administrateur sur une machine tant que celle-ci exécute une fonction réseau virtualisée traitant du trafic client ou des données sensibles. Au niveau OpenStack, cela passe par la définition de profils autorisants tous les appels API nécessaires à un type d'exploitant donné et bloquant ceux qui ne le sont pas. Cette configuration doit se faire au niveau de tous les services OpenStack utilisés. Pour simplifier ce travail, le groupe Orange est fortement impliqué dans le développement du projet Moon [8] qui vise à permettre la centralisation de la gestion de ces droits. Mais, même avec ces outils, au vu du nombre de commandes système et d'appels API disponibles, le travail de référencement et le choix des droits est long et fastidieux et est amené à être revu régulièrement.

Les flux entre les différents composants et logiciels de l'infrastructure de virtualisation doivent être sécurisés via la mise en place de chiffrement. Ce chiffrement nécessite une infrastructure de gestion de clés (PKI). Une PKI doit donc être mise en place et être compatible avec les différents composants de l'infrastructure. De plus, il faudra mettre en place un processus de renouvellement et de révocation des certificats déployés sur tous les composants.

Pour protéger les données contenues dans les disques virtuels des fonctions réseaux virtualisées en confidentialité et intégrité, une solution de chiffrement des disques virtuels doit être mise en place. Les clés de chiffrement utilisées doivent être protégées. Pour cela, une solution de gestion des secrets contenus au niveau de l'infrastructure de virtualisation doit être déployée. Le choix pour Orange France se porte vers un Hardware Security Module (HSM) à déployer en parallèle de l'infrastructure de virtualisation. En dehors de la vérification de la sécurité du HSM en lui-même, il est indispensable de vérifier la bonne compatibilité de celui-ci avec la solution de virtualisation choisie.

Enfin, une chaîne d'intégration et de déploiement continu (CI/CD) permettant une gestion des mises à jour des différents composants est également indispensable pour le maintien opérationnel de l'infrastructure. Cette chaîne doit également permettre des retours arrières rapides sur tous les composants en cas d'incident suite à une mise à jour. Etant donné la criticité de ces fonctions, il faut faire attention à ce que la mise en place de cette chaîne n'ajoute pas de nouvelles vulnérabilités en permettant un contrôle total du "Telco Cloud" par sa compromission et à ce que l'intégrité des composants soit toujours surveillée. De plus il faut bien avoir conscience que cette chaîne ne sera efficace qu'en complément d'un système de gestion des actifs de service et des configurations.

6 Supervision de sécurité

Les éléments cités dans le point précédent ne couvrent malheureusement pas tous les risques redoutés. Pour ces risques qui ne peuvent être couverts de manière proactive, une approche réactive s'appuyant sur une supervision de sécurité efficace peut constituer une réponse adaptée. Cela permet de ne pas rester démuni face aux risques non couverts et d'être en mesure d'agir avant que d'éventuels attaquants portent atteinte à la confidentialité ou à la disponibilité de la plate-

forme. Mais nous allons voir que le travail de mise en place sera long et fastidieux, notamment en raison de l'empilement de technologies hétérogènes utilisées, et de la faible maturité de ces solutions.

La supervision de sécurité est un complément aux mesures de protection dont l'objectif est de donner de la visibilité sur l'environnement et de valoriser les informations disponibles pour participer à la réduction du temps d'identification et de traitement des incidents de sécurité. Elle couvre les aspects suivants :

- mesure de la conformité (ce qui ne doit pas se produire par configuration ne se produit pas effectivement),
- détection des non conformités (pendant du point précédent),
- compensation partielle de l'absence de moyens de protection, d'une part via l'identification de l'occurrence de risques (événements craints) pour lesquels aucune mesure de protection n'est en place, et d'autre part via l'automatisation des ripostes en cas de détection d'événement constituant une alerte de sécurité,
- capacités d'investigation (centralisation des logs et moyens d'interrogation),
- visibilité sur l'environnement de contrôle.

Pour alimenter le SIEM (Security Information and Event Management) qui va réaliser la fonction de supervision de sécurité, il est nécessaire, au préalable, de collecter les logs des différents composants de l'infrastructure.

La collecte de ces logs constitue un changement d'échelle par rapport aux systèmes non virtualisés dû à :

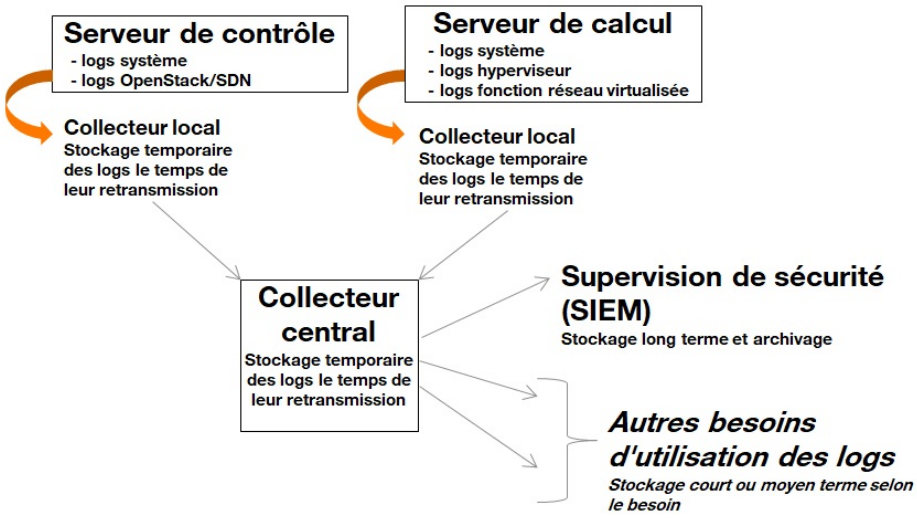
- l'augmentation des types de sources (et par conséquent de format et/ou sémantique),
- l'augmentation considérable de composants générant des logs : une infrastructure SDN/NFV va déployer un grand nombre de machines virtuelles pour réaliser les fonctions demandées, générant d'autant plus de logs.

Contrairement à des projets matures où l'on sait précisément quels types de logs sont intéressants pour la sécurité (que ce soit pour de la détection d'évènement ou de l'analyse post-mortem en cas d'incident de sécurité), il est beaucoup plus difficile dans le cadre des fonctions virtualisées de déterminer quels filtrages peuvent être opérés. Cela incite, au moins dans les débuts du projet, à injecter de grandes quantités de logs non filtrés ou très peu filtrés dans le SIEM, générant des besoins significatifs en terme de stockage et de capacité de traitement.

Dans ce contexte de fortes volumétries de logs à collecter, se pose également la question de leur archivage : quels logs conserver ? pendant combien de temps ? dans quel système ? Etant donné que des cas réels d'investigation post-mortem ne se sont pas encore présentés, il est difficile de déterminer quels logs présentent une véritable valeur, et lesquels peuvent être facilement filtrés. Concernant le lieu d'archivage des logs, le stockage associé au SIEM apparait comme le candidat naturel pour répondre à ce besoin : il permet en effet de garantir leur non-altération, ainsi que des capacités d'interrogations avancées.

En parallèle du besoin d'archivage des logs à des fins d'analyse sécurité, d'autres acteurs de la plateforme, notamment les exploitants, ont régulièrement besoin d'accéder à un certain niveau d'historique de logs. Afin de ne pas mélanger

ces besoins d'archivage et analyse de sécurité avec ceux de stockage de quelques jours, la stratégie adoptée est celle d'une collecte centralisée transitoire qui va ensuite redistribuer aux différents besoins, conformément au schéma suivant :



La collecte des logs étant effective, il devient alors possible de mettre en place des règles de détection. Parmi les règles pouvant être déployées de façon générique, on peut trouver :

- la détection d'attaques sur l'authentification (force brute, spraying, ...),
- la détection d'accès illégitimes ou non conformes (exemple : si les accès d'administration doivent provenir de bastions identifiés, on peut imaginer des règles qui alertent quand ce n'est pas le cas),
- la détection de dépassement de seuils sur certaines actions critiques (ex. usage d'API) – les seuils peuvent être fixes ou être sujets à une analyse continue,
- l'activation et/ou l'usage de fonctions normalement désactivées,
- la corrélation d'événements provenant de fonctions de sécurité (exemple : IDS/IPS déployés à des fin de détection de tentatives d'exploitation de vulnérabilités),
- le contrôle de la correcte application des rôles et les usages illégitimes des comptes génériques ou de services. Ces comptes ayant généralement des privilèges susceptibles d'intéresser un attaquant, il est très important de connaître ce qui en constitue un usage légitime (et donc les commandes associées) : tout usage de commandes hors de ce périmètre devra être identifié et traité comme un incident de sécurité.

Dans le cas de notre retour d'expérience, la fonction portée par la VNF existait déjà dans notre réseau sous la forme d'un équipement physique, dont le fonctionnement est strictement identique. Il était donc aisé, pour la supervision de sécurité de la VNF, de reprendre les règles de détections existantes.

Pour les composants nouvellement introduits (l'environnement OpenStack, la couche SDN, les cartes d'administration des serveurs...), la première étape

a consisté à couvrir les risques génériques (attaques par authentification, accès non conformes...), puis dans un deuxième temps à couvrir les risques spécifiques qui auront été identifiés.

L'expérience d'intégration des logs OpenStack (qui constitue le cœur de l'infrastructure de virtualisation) s'est révélée complexe et limitée, notamment en raison de l'absence d'une gestion unifiée. En effet, OpenStack ne se définit pas comme un produit global, mais comme un ensemble de composants qui, bien que fonctionnant de concert, constituent chacun un projet indépendant. L'une des conséquences de cette architecture est que, à l'heure actuelle, chaque composant (il en existe plusieurs dizaines) définit ce qui est loggué et comment, rendant très complexe voire impossible l'analyse d'un évènement, car il n'y a pas nécessairement de clé commune permettant de recouper les informations entre les différents composants.

Ces limitations constituent une problématique connue des communautés de développeurs OpenStack, qui travaillent à sa résolution ou tout du moins son amélioration. Il sera donc nécessaire d'étudier quelles nouvelles règles de détection pourront être mises en place lorsque le contenu des logs aura évolué.

De manière générale (et pour certains cas, à plus long terme), on cherche à détecter :

- que les VNF n'attaquent pas l'infrastructure (surveillance des API),
- que les VNF ne s'attaquent pas entre elles,
- que les VNF ne sont pas attaquées par l'extérieur,
- que l'infrastructure n'est pas attaquée de l'intérieur (règles sur le contrôle d'accès et sur les interfaces BMC (iLo, iDRAC...)),
- que l'infrastructure n'est pas directement exposée au monde extérieur et que, si elle l'est, elle n'est pas attaquée. Par exemple en vérifiant que les adresses IP source ou destination ne sont pas des adresses IP publiques,
- que l'infrastructure ne porte pas atteinte à la confidentialité des données des VNF, si elles sont sensibles (surveillance du respect du cloisonnement des droits). Exemple de règle : tentative d'accès au stockage par un compte non autorisé (même si l'accès échoue, l'existence d'une tentative qui est une non-conformité),
- que les interfaces d'administration ne sont pas utilisées à des fin malveillantes pour attaquer l'infrastructure ou les VNF. Exemple de règle : surveillance applicative pour détecter des actions privilégiées non autorisées.

Au-delà des logs des différents composants, il semble important d'être en mesure de déployer des moyens de détection d'intrusion et de surveillance des échanges réseau. Cependant, l'efficacité de ces moyens sera conditionnée à une intégration complexe à l'infrastructure de gestion de clés utilisée par la plate-forme OpenStack, étant donné que l'immense majorité des flux entre composants est chiffrée suite au renforcement sécurité effectué.

Dans le cadre de notre retour d'expérience, le nombre et la configuration des VNF est statique (pas encore de déploiement "à la volée"). Lorsque les déploiements de VNF seront dynamiques, il sera nécessaire de parvenir à une standardisation pour permettre leur intégration automatique à la supervision de

sécurité (une action manuelle serait chronophage et sujette à erreurs), et dans la même logique, le retrait automatique des composants supprimés. Un tel cycle de vie nécessite que la solution de supervision de sécurité présente des API dont l'usage devra être intégré à la chaine d'automatisation du SDN, ce qui présente un challenge supplémentaire.

Enfin, il est nécessaire d'anticiper les compétences des analystes du Security Operation Center concernant les technologies SDN/NFV, car il sera parfois nécessaire d'avoir une vue d'ensemble de la solution (et non pas simplement une agrégation de composants indépendants) lorsque certaines alarmes seront générées.

7 Conclusion

Les technologies SDN/NFV amènent de l'agilité et de l'automatisation dans le réseau mais le prix à payer est de devoir utiliser du matériel et des solutions logicielles non prévues pour une utilisation par un opérateur de communications électroniques et dont la stabilité risque de ne pas être au niveau attendu. Il faut donc tout d'abord que l'opérateur pallie les défauts de sécurité des solutions par du renforcement de sécurité. Ensuite, il doit compléter ce renforcement soit par des équipements périphériques ou des mesures spécifiques de sécurité lorsque cela est possible, soit par de la supervision de sécurité adaptée pour les autres cas. Il faut de plus noter que l'effort ne sera pas que technologique mais également humain car ce sera aux équipes d'ingénierie et d'exploitation de savoir s'adapter et adapter le réseau pour gérer cette transition en garantissant disponibilité et confidentialité.

References

1. Pascal Nourry, Franck Laurent : Contexte règlementaire pour les opérateurs 5G. In : Conférence C&ESAR 2019
2. Avis du CERT-FR CERTFR-2019-AVI-209, https://www.cert.ssi.gouv.fr/avis/CERTFR-2019-AVI-209/
3. Alexandre Gazet, Fabien Perigaud, Joffrey Czarny : Backdooring your server through its BMC : the HPE iLo4 case. In : SSTIC 2018
4. Nicolas Iooss : iDRACKAR, integrated Dell Remote Access Controller's Kind Approach to the RAM. In : SSTIC 2019
5. OpenStack Security Guide, https://docs.openstack.org/security-guide/
6. Liste des bugs du noyau Linux avec filtre sur KVM, https://bugzilla.kernel.org/buglist.cgi?quicksearch=kvm
7. Liste des bugs QEMU, https://bugs.launchpad.net/qemu
8. Projet Moon, https://git.opnfv.org/moon/