Le SD-WAN pour les nuls

Jérôme Durand

Cisco Systems
11 rue Camille Desmoulins
92782 Issy les Moulineaux
CEDEX 9

Résumé

La migration des applications dans le cloud et datacenters privés des entreprises amène à repenser fortement le WAN. Ce dernier évolue pour garantir la performance et la sécurité des applications. Des solutions dites "SD-WAN[1]"sont apparues ces dernières années, avec pour ambition de répondre aux nouveaux challenges apparus sur le WAN. L'architecture permet d'ajouter simplement sur chaque site une connexion Internet en plus des connexions WAN habituelles et d'utiliser chaque liaison de manière optimale. Le SD-WAN fait évoluer la mission du routeur : au-delà d'un transfert de paquets, il est maintenant en charge de router les applications pour garantir leur performance et leur sécurité. L'ONUG[2] a défini des critères permettant de qualifier une solution comme SD-WAN, afin d'aider chaque organisation à dissocier le bon grain de l'ivraie.

La mutation du WAN passe aussi parfois par l'empilement de boitiers, chacun résolvant une problématique particulière. Aussi la virtualisation des fonctions réseau se développe sur les sites distants. Il s'agit de ne configurer sur le site qu'un serveur x86 et de virtualiser chaque fonction sur ce dernier. Là aussi de nouvelles problématiques surgissent avec des différences fortes avec l'environnement en datacenter.

Cet article donne plusieurs clés de lecture, permettant d'étudier les différentes solutions SD-WAN et les challenges soulevés par la virtualisation des fonctions réseau.

Mots-clefs

SD-WAN, SDN, WAN, WAN hybride, Cloud, Overlay, contrôleur, NFV, NSH, service chaining

1 Introduction

Deux phénomènes amènent les réseaux WAN à devoir s'adapter. Il s'agit tout d'abord de la migration des applications vers le Cloud, en mode SaaS ou bien sur les datacenters privés des entreprises. Ce processus est souvent déjà engagé mais le nombre d'applications disponibles sous cette forme est tel que les effets de ce phénomène s'amplifient. Parmi les acteurs reconnus on trouve bien entendu Cisco Webex, Microsoft Office365, Google Apps, Salesforce mais aussi Workday ou Successfactors pour les ressources humaines, ADP pour la paie, vBrick pour la distribution de la vidéo différée ou Live. Dans la communauté RENATER, nous pouvons noter par exemple les services PARTAGE ou RENDEZ-VOUS, respectivement pour la messagerie et la web-conférence.

D'autre part, les organisations métiers demandent la mise en place de nouveaux services sur les agences, magasins, sites de production… Ces services digitalisent les sites distants et amènent de nouveaux usages comme le « guest access », c'est-à-dire la fourniture de connectivité WiFi aux clients ou autres personnes de passage, la distribution de la vidéo pour des usages variés (écrans, formation, évènements internes en direct), des applications portées sur tablettes ou smartphones…

[1] Software-Defined WAN
[2] Open Networking User Grou

A ces deux catégories de phénomènes s'ajoute l'augmentation de la consommation des ressources Internet depuis le poste de travail pour des usages professionnels mais aussi loisir. Le réseau doit donc être redéfini pour absorber ces nouvelles tendances :

- visibilité applicative et gestion des performances par application ;
- gestion de plusieurs accès WAN en mode actif-actif ;
- possibilité d'accéder à l'internet directement depuis le site distant sans repasser par le datacenter.

Le WAN évolue donc plus que jamais pour permettre de garantir performance et sécurité des applications, bien au-delà de la simple connectivité. Le SD-WAN (Software-Defined WAN) est la réponse affichée à ces tendances observées. Il est question de mettre le WAN au service des applications, tout en simplifiant son management.

2 Une définition pour le SD-WAN ?

C'est en 2014 environ que la terminologie SD-WAN commence à devenir largement utilisé. Le nombre de constructeurs clamant offrir une solution SD-WAN décolle. Un groupe de travail est alors formé au sein de l'ONUG (Open Networking User Group) pour rassembler les différents acteurs de la communauté SD-WAN.

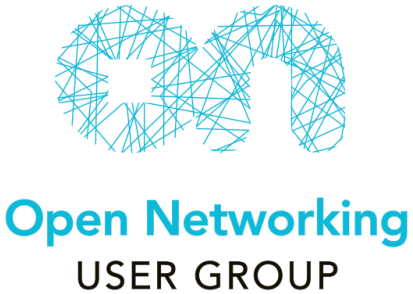

Figure 1 - Logo de L'Open Networking User Group (ONUG)

Ce groupe a permis de définir plus précisément le SD-WAN, afin de remettre un peu d'ordre et permettre aux organisations de s'assurer qu'une solution est en effet de type SD-WAN ou alors s'il s'agit d'un abus de langage d'une équipe marketing peu respectueuse de l'état de l'art.

2.1 Définition générale du SD-WAN selon l'ONUG

L'ONUG définit clairement les cas d'usage pour le SD-WAN et met au premier plan le besoin de baisser les coûts associés au WAN en tirant profit de l'Internet. Il s'agit de mettre en œuvre une architecture WAN hybride où une connexion Internet complète la connexion WAN privée traditionnelle sur le site distant. Cette connexion Internet a 2 objectifs :

- avoir un accès direct aux applications hébergées dans le cloud ;
- offrir un second lien entre le site distant et le site principal ou datacenter de l'organisation.

Sur cette connexion Internet un tunnel sécurisé est construit. Les applications sont dynamiquement routées sur les 2 liaisons (liaison privée et tunnel sécurisé sur Internet) en tenant compte de la performance des liaisons, de l'utilisation des liens.

La mise en place de liaison Internet permet ainsi selon l'ONUG de diminuer les coûts globaux de connexion, tout en restant maître des SLA[3].

[3] Service Level Agreement

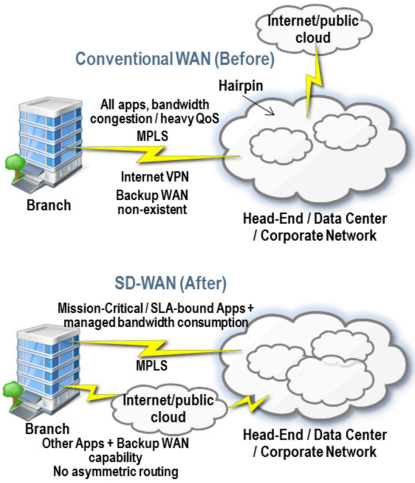

Figure 2 - SD-WAN (avant et après)[4]

Le SD-WAN fait évoluer la mission du routeur : au-delà d'un transfert de paquets, il est maintenant en charge de router les applications pour garantir leur performance et leur sécurité.

Au-delà de la mise en place d'une architecture hybride, le SD-WAN a comme postulat que la solution doit être simple à déployer pour une organisation, et ne doit pas être réservée aux opérateurs, experts du WAN. Aussi des interfaces de management simples caractérisent le SD-WAN, avec la possibilité d'offrir une abstraction du réseau.

2.2 Les 10 critères d'une solution SD-WAN selon l'ONUG

Le groupe de travail SD-WAN de l'ONUG va même jusqu'à créer une "SD-WAN requirement sheet", document Excel permettant simplement d'évaluer la conformité d'une solution d'un constructeur au SD-WAN. Dans ce document 10 points sont listés et sont explicités ci-dessous :

1. Gestion de plusieurs liens actifs (publics et privés)

Contrairement à un routage traditionnel qui va gérer les liens en partage de charge simple (ECMP[5]) ou en mode actif/passif, il doit être possible ici de répartir intelligemment le trafic sur divers liens en tenant compte de leur utilisation réelle. L'objectif ici est de permettre d'utiliser le maximum de la capacité disponible.

2. WAN construit sur des équipements physiques et virtuels

La virtualisation des fonctions réseau sur les sites distants est une nouvelle tendance qui a gagné en maturité et qui risque de s'accélérer ces prochaines années. Aussi un chapitre complet est dédié à cette thématique dans la suite de cet article.

3. WAN hybride sécurisé permettant d'appliquer une ingénierie de trafic par application, prenant en compte la performance des liens

L'interconnexion des sites doit pouvoir être faite sur tout type de transport et les connexions doivent être systématiquement chiffrées. Un "overlay", réseau virtuel à base de tunnels chiffrés (aussi appelé VPN) est construit sur les infrastructures physiques, masquant les disparités entre ces dernières.

Des règles d'ingénierie de trafic doivent pouvoir être mises en œuvre sur cet "overlay". A ce jour la plupart des organisations souhaitent continuer à router les applications critiques et temps réel sur les liaisons WAN traditionnelles (réseau MPLS-VPN) et router le reste sur les liaisons Internet à moindre coût. En cas de

[4] Source - page SD-WAN de l'ONUG - https://opennetworkingusergroup.com/software-defined-wide-area-network-sd-wan/
[5] ECMP - Equal Cost Multi-Path

problème de performance (par exemple une augmentation de la latence sur le lien MPLS-VPN) le trafic est automatiquement re-routé.

4. Visibilité et priorisation des applications critiques et temps réel selon les règles définies

Une solution SD-WAN doit reconnaître les applications, bien au-delà de simples ports TCP/UDP. On parle de DPI ou Deep Packet Inspection. Les règles de QoS sont appliquées sur les divers liens selon les applications.

5. Architecture hautement redondante

Plusieurs équipements SD-WAN doivent pouvoir être installés sur un site afin de pouvoir pallier la déficience de l'un d'entre eux. Un point clé à prendre en compte est l'architecture du datacenter qui est de loin l'élément le plus sensible.

6. Intéropérabilité au niveau 2 et 3 avec le reste de l'infrastructure

Les équipements SD-WAN doivent s'insérer dans tout type de réseau. A ce titre il est évident qu'ils doivent pouvoir communiquer en IP/Ethernet avec le reste de l'infrastructure (équipements du LAN de l'organisation et CPE opérateurs). A ce niveau on veillera à s'assurer que les équipements supportent l'ensemble des protocoles de routage afin de les insérer dans tout type de design (OSPF, BGP, IS-IS, EIGRP, HSRP, VRRP...)

7. Interface de management centralisée avec tableaux de bord par application, site et VPN

La visibilité applicative est souvent le premier élément souhaité par les organisations qui font un pas vers le SD-WAN. Avant même de mettre en place des redondances sophistiquées, une ingénierie de trafic ou des règles de QoS évoluées, il convient de savoir quelles applications transitent sur le WAN. Si la majeure partie du trafic sur un site est à caractère "récréatif", il sera simple de trouver une solution en priorisant les applications métier. En revanche si l'on s'aperçoit que la totalité du trafic est important pour l'organisation alors on s'orientera plutôt vers l'augmentation du débit, l'optimisation, et la mise en place de connexion directes vers l'internet si les applications sont fournies en SaaS.

8. Programmabilité de l'infrastructure à travers des API sur un contrôleur qui fournit une abstraction de l'ensemble. Envoi des logs vers collecteurs tiers (SIEM[6]...)

Le réseau SD-WAN doit interagir avec le reste de l'écosystème. Le contrôleur SD-WAN doit fournir des API permettant de mettre en œuvre des règles de routage, QoS... sans avoir à se connecter sur une interface graphique. Cela peut permettre d'insérer le SD-WAN dans les processus plus globaux appliqués sur l'ensemble du réseau (au-delà du WAN). Dans cet esprit il convient de s'assurer que les évènements remontés sur le WAN (logs...) puissent être exportés vers des collecteurs utilisés sur l'ensemble du réseau qui offriront une vision globale.

9. Un équipement doit pouvoir être déployé sans configuration et un minimum d'effort sur l'infrastructure actuelle

On parle de "zero-touch deployment" ou encore de "plug and play". L'objectif est de pouvoir pousser automatiquement un logiciel et une configuration sur un nouvel équipement SD-WAN installé. Il est important ici de s'assurer que les mécanismes utilisés vont au-delà du DHCP/TFTP ! Les échanges se faisant au-dessus d'une architecture WAN, on veillera à ce que les communications soient chiffrées et qu'il n'y ait pas de risque d'usurpation d'identité entre équipements SD-WAN (afin d'éviter qu'une personne malintentionnée récupère la configuration d'une organisation tierce).

10. Certification FIPS-140-2 pour le chiffrement

[6] Security Information and Event Management

Conformité de la solution sur des aspects sécurité.

2.3 Les points de vigilance

Le marché du WAN a largement évolué pour couvrir l'ensemble de ces problématiques. Chaque constructeur de solution spécifique (routage, firewall, optimisation WAN, DPI[7]/QoS[8], management, …) a fait évaluer sa solution ces dernières années pour tenter d'adresser l'ensemble de ces points. Le cadre défini par l'ONUG en 2014 est assez général et reste globalement valable à ce jour. Il offre cependant beaucoup de latitude aux constructeurs qui n'hésitent pas à qualifier leur solution de « SD-WAN » même si seulement quelques critères sont adressés !

Aussi, au-delà d'une application aveugle des travaux de l'ONUG, il est important de bien comprendre et prioriser les problématiques que l'on cherche résoudre pour mieux évaluer les diverses solutions proposées qui gardent souvent une spécialité, signature de l'origine de l'équipementier. Les points ci-dessous doivent susciter une vigilance particulière :

- Le coût : il reste certain que les liaisons restent de loin le poste de coût le plus élevé. Le gain du remplacement des liaisons WAN privées (liaisons louées, MPLS-VPN...) par des connexions Internet va fortement dépendre de la différence de prix entre ces 2 services. Ici nous avons des disparités très fortes selon les régions du monde. La France fait un peu office d'exception où il y a un faible écart de prix entre les liaisons Internet et MPLS chez les opérateurs. Le calcul du retour sur investissement est donc très variable d'une organisation à une autre et il convient de ne pas se contenter d'une étude provenant d'un cabinet de conseil américain.
- La sécurité : la mise en place d'une connexion Internet sur chaque site distant entraîne de facto de nombreuses questions sur la sécurité de l'infrastructure. Aussi il faut veiller à bien s'assurer que chaque mécanisme de sécurité soit robuste. Par exemple : vérification des algorithmes de chiffrement, vérification de la sécurité du mécanisme permettant le "zero-touch deployment"... De la même manière on veillera à bien comprendre comment la solution intègre des mécanismes de protection (firewall, IPS ou autres...) Les applications n'étant pas déployées sur les sites distants, les règles des dispositifs de sécurité restent le plus souvent simples et homogènes sur l'ensemble des équipements.
- Le cloud : tout comme les applications, le réseau lui aussi s'échappe parfois dans le cloud. Plusieurs solutions SD-WAN vont pouvoir profiter de solutions de management/contrôle fournies dans le cloud, accélérant et simplifiant le déploiement. Certaines solutions sont hybrides et peuvent être déployées dans le cloud ou encore au sein de l'organisation. Il est important de bien s'assurer du mode de déploiement des solutions et de s'assurer que celles-ci répondent aux critères de l'organisation, le plus souvent d'un point de vue sécurité.
- La migration : si la réalisation d'un test peut être simple, la migration de tout un WAN complet est toujours une opération nécessitant de nombreux points de vigilance. Comment les sites migrés en SD-WAN communiquent avec les sites non-migrés ? Comment la solution SD-WAN s'insère-t-elle dans le réseau ? La capacité de supporter de nombreuses options en termes de protocoles de routage est importante pour s'adapter à chaque infrastructure. Aussi le WAN intègre souvent de nombreux cas particuliers qui ont dû être déployés au fur et à mesure des années. La capacité de mettre en place des exceptions est primordiale pour s'adapter où cela est nécessaire, tout en gardant quand cela est possible une démarche d'harmonisation du design.

[7] Deep Packet Inspection
[8] Quality of Service

Il est important de bien mesurer ces différents aspects avant de lancer dans une refonte du WAN. Le rôle de ce dernier est toujours plus crucial et la mise en œuvre d'une nouvelle architecture ne doit pas altérer sa sécurité et sa disponibilité. Notons aussi que d'autres transitions sont en cours sur le WAN.

3 La virtualisation des fonctions réseau sur les sites distants

3.1 Quelle problématique ?

Si l'on ouvre une baie réseau d'un site distant, on trouvera souvent bien plus qu'un simple routeur d'accès. Des firewalls, IPS[9], solutions d'optimisation WAN, des solutions DDI [10]ou même de simples services locaux sont souvent installés. Parmi ces derniers on trouve des serveurs de fichiers, serveurs d'impression, solutions monétiques, solutions de vidéosurveillance ou encore de simples serveurs Linux ou Windows utilisés pour résoudre des incidents ou d'autres services.

La mise en place du SD-WAN (au sens décrit préalablement) n'est souvent qu'une des 2 grandes réflexions actuelles observées sur le WAN. De nombreuses organisations veulent aussi simplifier l'ensemble du dispositif. La multiplication des "boitiers" sur les sites distants entraîne des coûts opérationnels important et des délais (livraison, installation physique) et aussi une augmentation de la complexité et des designs non fonctionnels (par exemple un IPS aurait du mal à détecter des menaces si celui-ci est déployé en aval d'une solution d'optimisation WAN qui compresse les données).

Pour simplifier le réseau, une option qui devient de plus en plus considérée est la virtualisation des fonctions réseau (NFV[11]) sur le site distant. Au lieu de déployer de multiples boitiers, un serveur x86 sera installé (ou plusieurs si besoin de redondance) et les fonctions attendues seront virtualisées sur cette infrastructure. Les intérêts sont les suivants :

- Le déploiement d'une nouvelle fonction ne nécessite aucune opération logistique, d'opération d'installation coûteuse, ni de contrainte douanière ! Il suffit de charger l'appliance virtuelle sur le site distant et une nouvelle fonction peut être disponible immédiatement.
- Le design est simplifié puisqu'il n'y a plus de contrainte physique de connexion des équipements. S'il faut modifier ou adapter une infrastructure réseau (par exemple pour replacer l'IPS en amont de l'optimisation WAN) cela peut se faire en quelques clics sans recâblage.

Globalement le coût global du WAN peut être largement diminué tout en le rendant plus dynamique. L'intérêt est aussi de pouvoir faire face ponctuellement à des problématiques sur tout ou partie des sites. Si un évènement devait nécessiter sur un site une transmission vidéo et la mise en place d'une solution ad-hoc, il devient possible de s'appuyer sur l'infrastructure de virtualisation en place. La capacité de retirer cette solution une fois la diffusion terminée permet aussi d'envisager d'autres modes d'acquisition (abonnement à l'heure d'utilisation par exemple !)

3.2 Le "service chaining[12]"

Le développement de la virtualisation des fonctions réseau, en datacenter comme sur les sites distants, a mis en évidence le besoin de pouvoir chaîner aisément les fonctions réseau.

Prenons l'exemple d'un design assez classique qui nécessite qu'un paquet transite d'abord par le routeur SD-WAN, puis par un firewall, ensuite par une solution d'optimisation WAN avant de revenir par le routeur SD-WAN pour être chiffré avant d'être envoyé sur le WAN. Il convient tout d'abord de placer les différentes fonctions dans le bon ordre. Il serait en effet difficile de scruter un paquet au niveau du firewall si celui-ci

[9] Intrusion Prevention System
[10] DNS, DHCP, IPAM (IP Address Management)
[11] Network Function Virtualization
[12] Enchaînement de Services

était placé après un mécanisme d'optimisation WAN, qui compresse les paquets et modifie largement la gestion de TCP !

Dans un monde où chaque solution est déployée sous forme "d'appliance" physique, le séquencement des opérations est assez simple puisqu'il va suivre le câblage, via des opérations de routage ou commutation traditionnelles. Chaque boitier va traiter le paquet et l'acheminer au suivant après traitement.

Les designs virtualisés aujourd'hui tendent à reproduire plus ou moins ces mêmes méthodes compte tenu de l'absence d'alternative. Des VLAN sont implémentés entre les différentes VNF [13]et une chaîne est faite en aboutant statiquement les éléments entre eux. Cette solution, bien que fonctionnelle, ne répond pas intégralement aux objectifs d'un réseau virtualisé :

- La virtualisation a pour objectif de simplifier l'ajout / la suppression de fonctions réseau. Il convient donc de s'assurer que des contraintes réseau ne viennent pas gâcher cette flexibilité souhaitée.
- Comme les solutions partagent des ressources physiques communes (processeurs, mémoires...) on va d'autant plus chercher à optimiser le traitement des paquets. Pour cela on va s'assurer qu'une même opération ne soit pas faite sur plusieurs VNF. Dans l'exemple précédent, on peut concevoir qu'une fonction DPI soit implémentée sur le routeur SD-WAN, mais aussi sur le firewall et la solution d'optimisation. Des solutions doivent permettre d'éviter de répéter une opération si coûteuse en ressources.

Afin d'avancer sur le "service chaining", le groupe de travail IETF[14] sfc (Service Function Chaining) a été créé. La problématique complète ainsi qu'une architecture ont été définis dans les RFC 7498 et 7665.

Les flux sont tout d'abord pris en charge par un "Service Classifier" (SC) et sont ensuite acheminés entre "Service Function Forwarders" (SFF) qui à leur tour vont successivement appeler des "Service Functions" (SF).

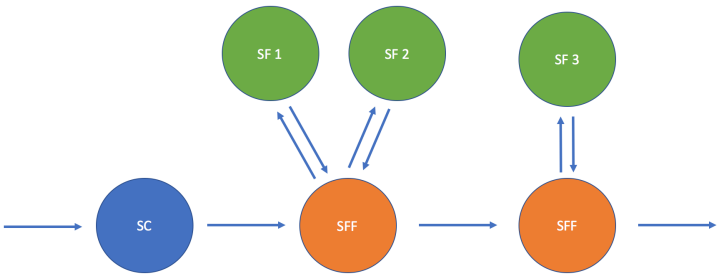

Figure 3 - Service Function Chaining - Architecture simplifiée

Bien évidemment, différentes fonctions peuvent être portées par une seule et même VNF. Par exemple, le routeur SD-WAN pourra être à la fois Service Classifier, puis le SFF qui appellera des Service Functions présentes sur d'autres VNF.

L'architecture laisse libre le mécanisme permettant de faire transiter les paquets entre SFF et SF. Par exemple, des tunnels VXLAN ou GRE pourront permettre une communication simple au-dessus d'une infrastructure IP : plus besoin d'abouter des VLANs. L'ajout d'une nouvelle SF (par exemple un proxy web) se fera simplement en déclarant une nouvelle SF au niveau du SFF voulu.

Par contre, un nouveau protocole appelé NSH (Network Service Header) a été conçu pour permettre une communication au niveau service des éléments entre eux. Un en-tête NSH est ajouté aux paquets et va propager notamment le Service Path Indentifier déterminé au niveau du SC, qui sera utilisé sur chaque SFF pour appeler successivement les différentes SF. Le protocole NSH est hautement flexible et permet de

[13] Virtual Network Function (fonction réseau virtualisée)
[14] Internet Engineering Task Force

transporter tout type de metadata, caractérisant mieux le service et/ou le flux. Un application-ID peut par exemple être ajouté par la première SF qui fera du DPI, et pourra être ensuite consommé par les SF suivantes qui n'auront plus à déterminer l'application transportée.

Afin de paramétrer tous les éléments de la chaîne dynamiquement depuis un contrôleur central, un plan de contrôle NSH est également en cours de définition à l'IETF.

Il est peut-être un peu tôt pour espérer avoir des solutions offrant un service chaining intégralement dynamique et optimal compte tenu de la jeunesse relative de la standardisation de NSH à l'IETF. Cependant il semble indispensable de prendre en compte dès aujourd'hui les plans d'intégration de NSH dans chaque solution de virtualisation. Quand un réseau hybride physique/virtuel est en place, il est important de vérifier que les ASIC ou autres Network Processors utilisés sont assez flexibles pour intégrer la gestion de NSH, protocole complexe à traiter du fait de sa très haute dynamicité.

3.3 Les points de vigilance

La virtualisation est souvent largement utilisée dans les datacenters sur les applicatifs, et peut sembler être acquise et bien comprise. Cependant, quand il s'agit de virtualisation de fonctions réseau sur les sites distants il y a quelques particularités à prendre en compte, du hardware jusqu'aux mécanismes d'orchestration.

- Format du serveur : tout d'abord le serveur x86 doit être choisi en tenant compte des critères environnementaux spécifiques aux sites distants, souvent très éloignés des salles blanches rencontrées en datacenter. Les baies sont parfois moins profondes (baies télécom de 60 cm) et il arrive qu'il n'y en ait même pas. La climatisation est parfois moins efficace et l'alimentation électrique plus incertaine. Nous avons aussi davantage de risques de vibrations, de chocs qui pourraient être dus à des livraisons et installations faites sans grand respect pour les règles de l'art. Pour toutes ces raisons la facture du serveur et son "durcissement" doivent être pris en compte. Notons aussi que le bruit généré par le serveur doit être étudié. Dans de nombreux cas, les équipements réseau ne sont pas dans un local technique et doivent cohabiter avec des individus qui aspirent à travailler en paix.
- Connectivité WAN : si la connectivité en datacenter est faite de multiples ports 10 GigabitEthernet ou plus, la connectivité sur les sites distants est beaucoup plus variée. Un bon nombre d'organisations aujourd'hui opte pour des connexions LTE ; et la technologie DSL est aussi largement utilisée dans nos contrées. Il faut s'assurer de la compatibilité du serveur avec ces technologies de transport si aucun modem tiers n'est en charge de la conversion entre l'Ethernet interne vers la technologie de transport utilisée sur le WAN.
- Simplicité de déploiement : un autre aspect qui mérite d'être étudié est la capacité de déployer simplement le serveur directement sur le site distant, sans opération préalable de "staging" sur un site ad-hoc. En bref, tout comme pour la brique SD-WAN présentée préalablement, il doit être possible de démarrer un serveur, d'instancier des VNF, et de les configurer sans aucune opération manuelle autre que quelques branchements électriques et réseau. Les opérations se faisant au travers du WAN (et même éventuellement au travers d'une connexion Internet) une vigilance doit être portée sur la sécurité associée à tous les mécanismes dits de "zero-touch deployment".
- Performance : il est également intéressant de considérer la différence des flux entre les VM[15] sur un datacenter, et les VNF sur les sites distants. En datacenter, un flux entre sur un serveur, est traité par une VM puis est éventuellement transféré sur une autre VM qui sera le plus souvent sur un autre serveur : les flux sont ici principalement nord/sud (du réseau vers les VM). Dans le contexte d'un site distant, les flux transitent entre VNF sur un même serveur. Un paquet, qui doit être acheminé en un minimum de temps, doit être traité successivement

[15] Virtual Machine (machines virtuelles)

par de nombreux processus sur un même équipement. Chaque paquet reçu génère des interruptions CPU à la fois au niveau de l'hyperviseur mais également au niveau de la VNF. Cela est d'autant plus critique que l'on va généralement chercher à dimensionner les processeurs x86 au plus bas sur les sites distants pour diminuer les coûts. Depuis de nombreuses années, SR-IOV permet d'optimiser la performance pour les flux rentrant sur un serveur : la carte d'interface réseau va pouvoir présenter directement un paquet à la VM sans nécessiter un traitement au niveau de l'hyperviseur, sauvegardant largement les ressources. Dans un contexte de flux est-ouest (trafic entre VM d'un même serveur), il est intéressant de considérer les mécanismes équivalents pour optimiser les flux entre machines virtuelles. Sur cet aspect des solutions commencent à peine à émerger et sont très liées au matériel.

- Management : un autre aspect intéressant à prendre en compte est la technologie de management de l'hyperviseur. Dans un datacenter, il existe une bande-passante infinie entre un hyperviseur et l'entité qui assure son management, avec une latence quasi nulle. Les performances de la connexion de management sont excellentes et déterministes. Notons aussi que de nombreuses connexions redondantes sont en place et des réseaux complets dédiés au management sont configurés. Même en cas d'intervention sur le réseau, l'hyperviseur reste le plus souvent joignable de son manager. Cependant dans le WAN c'est toute une autre histoire : aucune organisation ne pourra s'offrir le luxe de déployer un WAN 10GE uniquement pour manager les serveurs déployés sur chaque site. La solution de management de l'hyperviseur doit permettre par exemple une mise à jour du routeur virtuel du site qui déconnecterait le temps de l'opération l'hyperviseur de son orchestrateur.
- Ouverture : il est important que la solution en place permette d'instancier tout type de VNF et non seulement celles de quelques constructeurs. On veillera à s'assurer de l'ouverture de la solution à des standards en la matière. A titre d'exemple Linux KVM offre cette ouverture. D'autres technologies de virtualisation permettent également de virtualiser un large panel de VNF.
- Intégration dans l'écosystème réseau : contrairement aux serveurs et VM qui sont déployés dans les datacenters, gérés le plus souvent par des équipes dédiées aux serveurs, les serveurs déployés pour virtualiser les fonctions réseau sur les sites distants sont le plus souvent managés par les équipes réseau qui ont su évoluer. Cependant ces dernières cherchent à intégrer au maximum les nouvelles briques dans l'infrastructure de management réseau en place. Des protocoles de management réseau (comme par exemple Netconf/RESTconf, SNMP, syslog ou encore la CLI) sont souvent privilégiés par les équipes réseau qui doivent retrouver dans ces nouveaux systèmes des automatismes largement maîtrisés depuis de nombreuses années.

Si la virtualisation des fonctions réseau est prometteuse, et si de nombreuses organisations et opérateurs se lancent dans l'aventure, il convient de mesurer les gains réels et de ne pas mettre en danger le WAN si tous les aspects ne sont pas bien maîtrisés.

4 Conclusion

Derrière une appellation SD-WAN souvent trop appropriée par les équipes marketing se cache de réelles problématiques techniques. Le WAN évolue enfin pour s'adapter à la mutation des applications. Cependant il convient de rester vigilant car le WAN doit avant tout être robuste et sécurisé. La mise en place de solutions innovantes ne peut donc se faire sans une intégration dans l'écosystème en place (réseau, supervision, management...) Les critères définis par l'ONUG sont une bonne base de départ pour évaluer une solution SD-WAN mais doivent être complétés par une analyse poussée directement liées aux problématiques de chacun.

Cette évolution vers le SD-WAN accentue une autre mutation : la virtualisation des fonctions réseau sur les sites distants. Là aussi des solutions commencent à devenir mûres pour un déploiement en production. Cependant il convient là aussi de ne pas oublier les spécificités liées à l'environnement des sites distants,

très loin des contraintes des datacenters. Au-delà des avantages certains offerts par la virtualisation il faut prendre en compte comment elle peut s'insérer dans les processus opérationnels actuels bien rôdés.

Bibliographie

Halpern, J., & Pignataro, C. (2015). RFC 7665 - Service Function Chaining (SFC) Architecture.

Quinn, P., & Nadeau, T. (2015). RFC 7498 - Problem Statement for Service Function Chaining. *IETF*.

Quinn, P., Elzur, U., & Pignataro, C. (2017). draft-ietf-sfc-nsh-20 - Network Service Header (NSH).

SD-WAN, O. -g. (2014, 01 01). *SD-WAN Working Group*. Récupéré sur Open Networking User Group: https://opennetworkingusergroup.com/software-defined-wide-area-network-sd-wan/

SD-WAN, O. -g. (2014, 1 1). *SD-WAN-Requirements-Sheet*. Récupéré sur Open Networking User Group: https://opennetworkingusergroup.com/wp-content/uploads/2015/05/FINAL-SD-WAN-Requirements-Sheet.xlsx