LIVRE BLANC
RÉSEAUX HYBRIDES ET CLOUD COMPUTING

T · · Systems ·

TABLE DES MATIÈRES

RÉSEAUX HYBRIDES D'ENTREPRISE : INTRODUCTION

Les applications cloud font l'objet d'une demande croissante de la part des particuliers et des professionnels. Le modèle hybride combine des ressources de clouds publics et privés. Cette approche change fondamentalement la conception et la gestion des réseaux d'entreprise, le cloud hybride nécessitant également une infrastructure réseau hybride.

Jusqu'à présent, les applications hébergées sur des data centers d'entreprise et des clouds privés étaient clairement séparées des applications déployées dans le cloud public. Chacune était déployée en fonction des exigences applicables en matière de sécurité et d'accessibilité des données. Le cloud hybride abolit cette séparation. Il permet la distribution dynamique des applications et des bases de données entre les data centers d'entreprise, et des environnements de cloud public ou privé (Figure 1). Les processus de calcul peuvent être répartis de manière dynamique en fonction des besoins fluctuants des entreprises. Public ou privé, le cloud est un moyen économique de faire évoluer ses ressources informatiques en les activant ou les désactivant dans des délais très courts selon la demande. La répartition d'applications sur plusieurs environnements hétérogènes permet d'équilibrer la charge de travail. Il est par ailleurs possible de créer une redondance entre plusieurs sites et environnements cloud lorsque la sauvegarde des données et la disponibilité élevée des applications sont essentielles.

Ces évolutions ont une incidence significative sur la structure des systèmes d'information d'entreprise. Les clouds publics et privés et les data centers doivent être bien plus intégrés à l'environnement réseau afin de pouvoir assurer un modèle de communication entre tous les sites avec des schémas et des profils d'utilisation qui changent de manière dynamique, mais aussi de répondre au besoin permanent d'accéder à Internet. Dans les architectures traditionnelles, l'Intranet était ancré sur des plates-formes de réseau privé. L'accès à Internet était en général contrôlé via une ou deux passerelles centrales dotées de politiques de sécurité restrictives. À l'avenir, Internet et les plates-formes privées, comme Ethernet et MPLS, devront être bien mieux intégrés pour garantir une communication fluide entre les environnements de cloud publics et privés. La nouvelle structure hybride est susceptible d'entraîner des schémas de trafic plus volatils, avec par exemple des pics de charge lorsque des machines virtuelles ou des bases de données sont copiées ou déplacées entre des data centers. Les nouveaux réseaux hybrides devront donc être en mesure de répondre à ce schéma dynamique et de répartir les charges de travail de façons aussi uniforme et économique que possible.

Le réseau hybride d'entreprise répond également à la demande croissante en bande passante. Il doit répartir le trafic conformément aux besoins des applications sur des structures de réseau de qualité et coûts inégaux (c'est-à-dire, une connectivité à haut et bas débit), dans le but de réduire les coûts tout en offrant la meilleure expérience possible à l'utilisateur final. Les réseaux hybrides prennent en charge le cloud hybride. Le marché du cloud évolue si vite qu'il entraîne une mutation du marché des technologies réseaux. En outre, pour la première fois en plus de dix ans, un nombre croissant de startups financées par des sociétés de capital-risque pénètrent sur le marché international de l'IP VPN pour contribuer à la création et à la croissance rapide des réseaux hybrides. Les fournisseurs de services réseau d'entreprise traditionnels devront réaménager leurs plates-formes et produits pour rester compétitifs à l'ère du cloud computing.

Le terme « réseau hybride » décrit en général la combinaison d'au moins deux types ou technologies de réseau, habituellement avec des exigences de sécurité différentes (c'est-à-dire, Internet et plates-formes privées). Les passerelles entre les différents réseaux sont installées dans le contexte d'un réseau d'entreprise (habituellement un par bureau) ou partagées au sein de la plate-forme réseau du fournisseur de services. L'objectif : faire en sorte que chaque flux de communication sur le réseau utilise le canal le plus rentable en fonction des exigences de sécurité et de qualité de service de chaque application.

Les réseaux de télécommunications hybrides peuvent combiner un certain nombre de plates-formes réseau différentes :

- des réseaux de fibre optique pour satisfaire à des exigences de bande passante très élevées, pour l'interconnexion de data centers par exemple ;
- Internet, avec toute une variété de types d'accès réseau possibles, tels (modem câble, DSL, ELT ou Ethernet) ;
- des réseaux Ethernet de plates-formes privées pour les liaisons haut débit de couche 2 ;
- une plate-forme privée IP VPN (la quasi-norme actuelle en matière d' environnements réseaux étendus d'entreprise) utilise le plus souvent la technologie MPLS sur la couche principale.

Ce livre blanc utilise exclusivement le terme « réseau hybride » pour faire référence aux réseaux qui combinent l'accès Internet à une plate-forme IP VPN privée (en général MPLS).

CAPACITÉ À PASSER DU CLOUD PRIVÉ AU CLOUD PUBLIC

Pouvez-vous mettre à disposition et/ou transférer des applications et données depuis votre cloud privé vers un ou plusieurs services cloud public tels qu'AWS, Azure, GCE ou SoftLayer ?

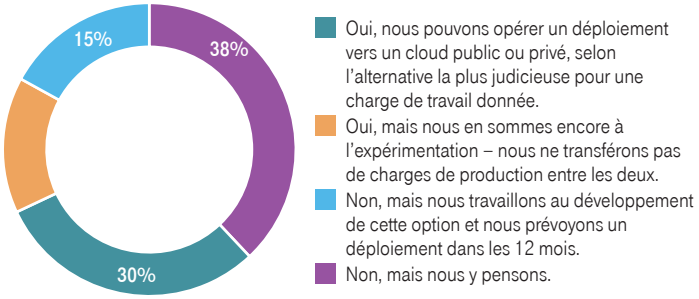


FIG. 1 : Utilisation du cloud hybride par les entreprises. Source : InformationWeek

SCÉNARIOS DE CLOUD HYBRIDE

Un cloud hybride combine des ressources opérées sur site et/ou dans un cloud privé avec des ressources hébergées dans le cloud public. Dans un environnement privé, les services de data center sont attribués à un client unique. De l'autre côté, le cloud public, comme son nom le suggère, est accessible au grand public. Des scénarios hybrides se produisent quand les processus de calcul et les bases de données du data center d'entreprise ou d'un environnement de cloud privé sont associés à des ressources publiques (par exemple, si le premier est migré vers le dernier). Le marché de l'hybride devrait progresser en moyenne de 30% par an jusqu'en 2018. À peu près la moitié des entreprises préparent déjà le terrain pour des scénarios de cloud hybride (Figure 2).

STRATÉGIE DE CLOUD D'ENTREPRISE

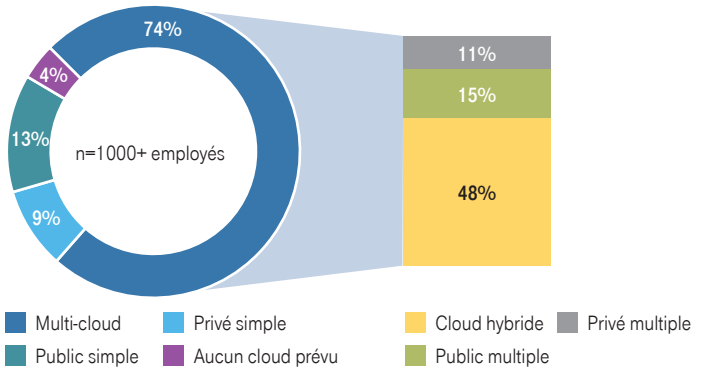


FIG. 2 : Stratégies de cloud d'entreprise, Rapport sur l'état de l'art du cloud.
Source : RightScale

La croissance est principalement portée par les économies potentielles réalisables. En général, il revient plus cher d'exploiter un data center sur site ou de payer l'accès à une infrastructure virtuelle privée que d'avoir accès à des ressources de calcul et de stockage comparables dans un cloud public. En outre, le modèle public offre davantage de flexibilité : il suffit d'activer et de désactiver les services cloud public normalisés pour augmenter ou réduire les ressources informatiques rapidement en fonction des impératifs. Le cloud privé, en revanche, offre une plus grande exclusivité et se veut une solution moins standard. Comme les serveurs du client sont exploités dans des data centers extrêmement sécurisés, cela se traduit également par davantage de sécurité (avec une protection renforcée contre l'accès non autorisé aux données et applications sensibles). Par ailleurs, les utilisateurs de clouds privés peuvent convenir de services supplémentaires avec leurs fournisseurs (par exemple, des niveaux de service et d'assistance améliorés ou une disponibilité plus élevée).

OBSTACLES AU CLOUD COMPUTING

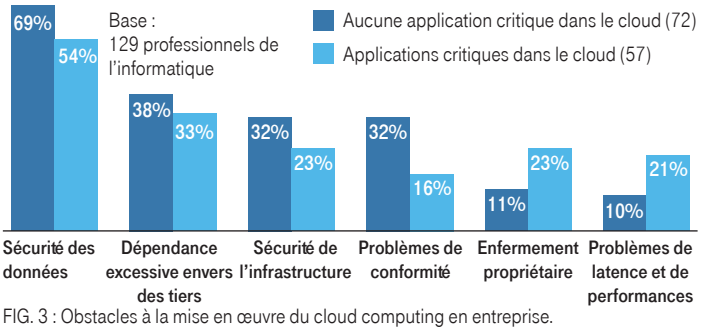


FIG. 3 : Obstacles à la mise en œuvre du cloud computing en entreprise.
Source : John Leonard

Toutefois, les entreprises cherchant à combiner le meilleur des deux mondes peuvent se trouver confrontées à un certain nombre d'obstacles (Figure 2). L'un d'eux est l'absence de mécanismes et règles de sécurité clairement définis pour le stockage et le traitement des données critiques dans les environnements externes. Autre problème : l'inquiétude des responsables informatiques quant à l'absence de SLA concernant la disponibilité des systèmes de cloud public. De nouvelles stratégies de sauvegarde et de redondance s'imposent pour garantir aux utilisateurs professionnels l'accès à des données et à des ressources de calcul d'une qualité identique à celle qu'ils recevraient de leur système informatique interne. En outre, les environnements de cloud hybride requièrent souvent des réseaux conçus pour garantir une disponibilité élevée et une faible latence. Dans un tel contexte, trois facteurs sont particulièrement importants :

1. La répartition des applications entre les divers types de cloud
2. La répartition géographique des applications
3. L'accès des utilisateurs au cloud

RÉPARTITION DES APPLICATIONS ENTRE LES TYPES DE CLOUD

Les applications peuvent être réparties entre divers environnements cloud. Habituellement, les applications non critiques sont transférées en intégralité vers le cloud public. Une base de données peut également être hébergée dans un environnement privé, pendant que le logiciel de traitement de données opère depuis un système public. Une troisième possibilité consiste à l'exploiter comme un système de secours : si le logiciel dans le cloud privé doit être inaccessible pour une raison quelconque, le cloud public peut prendre le relais. Des scénarios d'équilibrage de charge sont également envisageables.

ÉVOLUTION DU TRAFIC IP

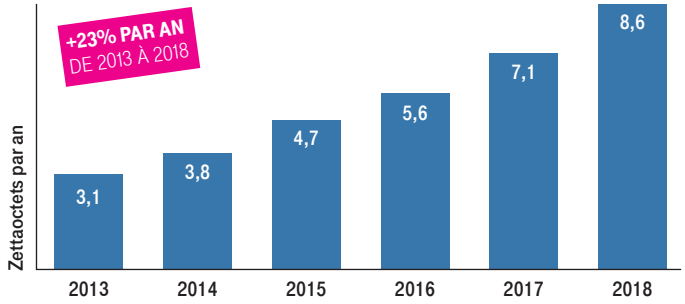


FIG. 4 : Trafic IP dans des data centers cloud. Source : Cisco

Ces cas d'utilisation ne sont pas figés ; ils mènent plutôt à une répartition dynamique des charges de travail entre les clouds privés et publics en fonction des besoins de l'entreprise.

Conséquence pour les réseaux : cela alimente la demande en bande passante (Figure 4), et impose également un double défi en matière de

ÉCHANGE DE DONNÉES SUR LES RÉSEAUX HYBRIDES D'ENTREPRISE

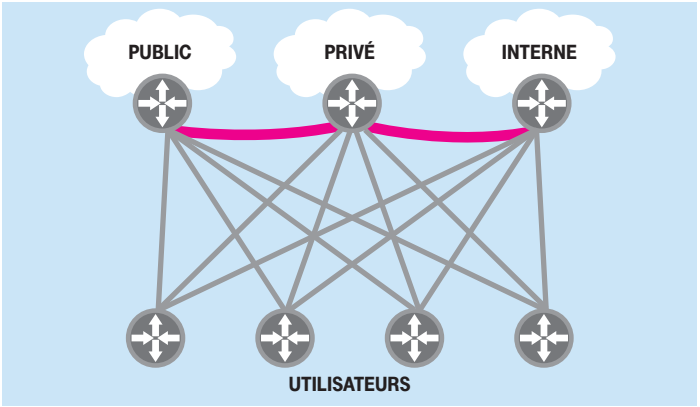


FIG. 5 : Connexions au sein des réseaux hybrides d'entreprise. Source : T-Systems

communication des données. En premier lieu, il est impératif d'assurer une vitesse de transfert élevée entre les bases de données et le logiciel, et de réduire la latence entre l'utilisateur et le serveur. Ensuite, il est essentiel d'être en mesure de répartir de manière dynamique d'importants volumes de données entre différents types de clouds (Figure 5).

RÉPARTITION DU TRAFIC IP

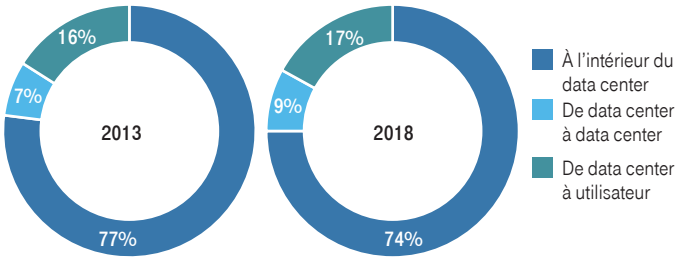


FIG. 6 : Répartition du trafic IP dans un data center cloud. Source : Cisco

Ces dernières années, la virtualisation des data centers a déjà conduit à une augmentation substantielle du trafic croisé entre clouds, principalement pour la mise en œuvre de politiques de sauvegarde (Figure 6). Cette tendance devrait également toucher le trafic inter-cloud, car les charges de travail sont réparties de manière dynamique entre plusieurs environnements cloud afin de répondre aux problématiques d'accessibilité des environnements cloud.

RÉPARTITION GÉOGRAPHIQUE DES APPLICATIONS DANS LE CLOUD

Les analystes ont eu tendance à classer les fournisseurs de réseaux d'entreprise selon le nombre de PoP exploités dans le monde. Ce postulat s'appuie sur le fait que, quand le nombre de nœuds augmente, le coût d'accès moyen baisse pour le client. Une situation similaire émerge désormais concernant l'expansion des ressources de calcul. Si les clients potentiels se situent physiquement à proximité des data centers d'un fournisseur de services cloud, les frais d'accès sont faibles. Lorsque des succursales situées en Asie du sud-est se connectent à des systèmes de cloud à Singapour, et que d'autres à l'est des États-Unis et du Canada accèdent à des ressources à New York, la latence est maintenue au minimum. Toutefois, les jeux de données qui résident dans plusieurs régions doivent être synchronisés (ce qui augmente encore les volumes de trafic de données sur les réseaux).

Les solutions de sauvegarde et de reprise d'activité sont des éléments cruciaux pour assurer la continuité opérationnelle des data centers. Si des applications ou des bases de données hébergées sur le data center principal ne sont plus accessibles (malgré la redondance interne) la configuration de sauvegarde créée dans un second data center et à emplacement géographique différent prend le relais. Pour une bascule fluide, il est nécessaire de synchroniser les données en permanence sur le site de sauvegarde (et de vérifier que la connexion réseau peut supporter l'afflux des volumes de données quand il a lieu).

Quand une entreprise cliente commande des ressources de stockage ou de calcul, le fournisseur cloud demande généralement des détails sur la structure géographique de l'entreprise (travaillant ainsi avec le client pour décider quel data center est le plus approprié. Les utilisateurs gardent ainsi le contrôle sur l'endroit où sont stockés leurs données et processus de calcul. Pour les fournisseurs, en revanche, cela peut être moins avantageux, car ils sont limités au moment d'harmoniser les architectures cloud entre plusieurs data centers et de fournir un accès fluide au cloud dans des contextes internationaux.

Ceci étant, le nombre de data centers par fournisseurs cloud est limité et tend à diminuer. La Figure 7 montre les data centers proposés par Equinix (chiffres valables pour 2016). Equinix est l'un des principaux fournisseurs d'infrastructure globale pour la connexion de ressources de calcul avec des WAN. Il a créé des passerelles vers tous les grands fournisseurs cloud et propose à ses clients un accès normalisé à ces ressources via sa propre plate-forme. À ce titre, la carte en figure 7 peut être considérée comme représentative de la répartition mondiale des data centers cloud. Elle permet de tirer trois conclusions :

1. La part de ressources de calcul la plus importante se trouve en Europe de l'ouest et aux États-Unis. Une recherche sur Google confirme cette conclusion. Par ailleurs, la plupart des fournisseurs de services cloud on leur siège aux États-Unis.

RÉPARTITION DES DATA CENTERS ET DES SERVICES DE CO-IMPLANTATION EQUINIX

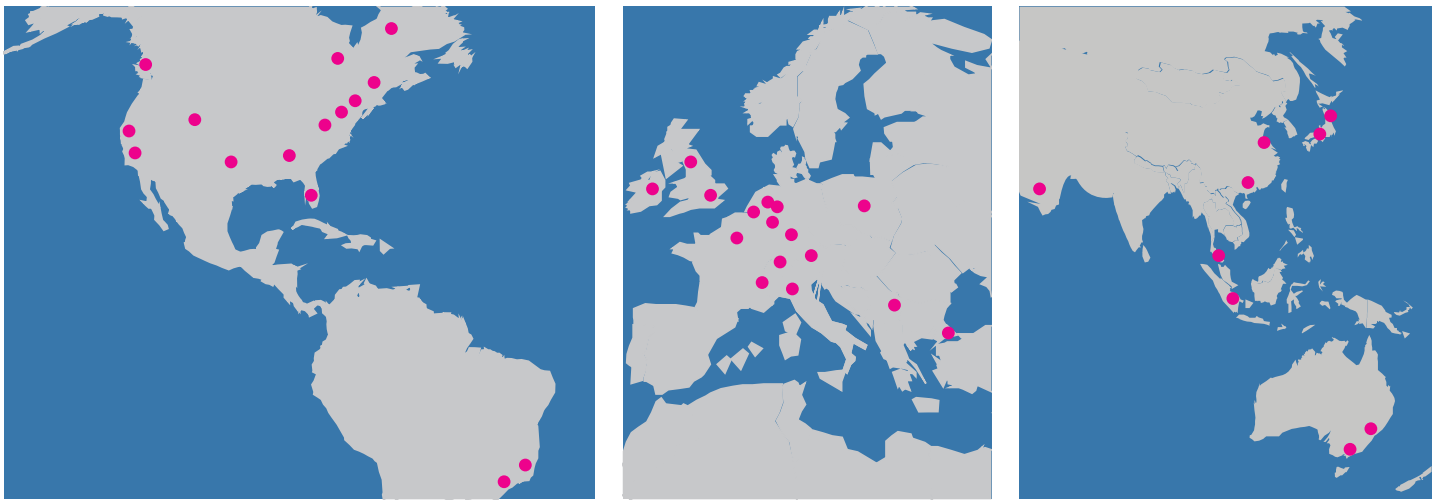


FIG. 7 : Les ressources des data centers virtuels destinées à différentes unités administratives viennent de pools de clouds. Source : Equinix

2. En dehors de l'Europe de l'ouest et des États-Unis, les ressources de calcul de chaque pays sont concentrées sur un site ou dans un faible nombre de sites.
3. Seules les économies solides et établies disposent de ressources de calcul.

Une vraie opportunité pour les fournisseurs de services réseau partout dans le monde, qui ont besoin de moins de points d'interconnexion. Ces points d'interconnexion sont généralement mis en œuvre là où le fournisseur possède un ou plusieurs gros nœuds réseau opérationnels. Ainsi, pour l'opérateur de réseaux, il faudra toujours se connecter à plusieurs fournisseurs de services cloud dans deux ou plusieurs sites en Europe de l'ouest et aux États-Unis, puisque la majorité du trafic issu du cloud public provient de là, et qu'au minimum deux passerelles sont nécessaires par cloud afin d'assurer des temps de latence acceptables. Il faut également prévoir au moins une passerelle en Asie du sud-est. En fait, les grands opérateurs de services réseau mettent généralement en œuvre au minimum trois de ces passerelles afin de connecter trois principaux centres : en Australie (Sydney ou Melbourne), au Japon (Tokyo), à Singapour ou en Indonésie (Jakarta). Le dernier centre important à prévoir en matière de data centers (et le seul dans la région) doit être créé au Brésil (Sao Paolo ou Rio de Janeiro).

ACCÈS DES UTILISATEURS AUX APPLICATIONS DANS LE CLOUD

Pour les utilisateurs de ressources cloud au quotidien, les principales priorités sont la disponibilité des applications, la vitesse et la fiabilité des temps de réponse. Ces facteurs doivent être pris en compte lors de la conception des réseaux et de la répartition dynamique des processus et des données sur plusieurs environnements cloud.

Avec la mobilité croissante des employés et toujours plus de connexion Internet haut débit, nombre d'entreprises ont étendu leur réseau pour permettre la connectivité mobile. La demande en applications cloud comme WebEx, GoToMeeting et Office 365 en dehors du bureau a augmenté. Sur un réseau d'entreprise conventionnel, les employés qui travaillent depuis leur domicile ou en déplacement se connectent à une plate-forme de réseau privé (et à l'Intranet de l'entreprise) depuis Internet, au moyen d'une ou plusieurs passerelles Internet sécurisées. Cela permet aux utilisateurs d'avoir accès aux données internes de l'entreprise et, s'ils y sont autorisés, aux applications sur l'Intranet via une instance de sécurité centralisée et relativement facile à contrôler (Figure 8).

Toutefois, cette conception de réseau conventionnelle devient rapidement obsolète dans ce nouveau monde hybride et dynamique – les passerelles Internet centralisées deviennent vite des goulots d'étranglement qui limitent le rendement des utilisateurs adeptes du télétravail ou en déplacement. La tendance actuelle exige de nouvelles approches en termes de latence du réseau et de connectivité mobile. Par exemple, des méthodes autorisant l'accès à un ordinateur ou smartphone d'un utilisateur, ou sélectionnant à chaque instant le meilleur réseau disponible.

Bien que les réseaux de communications Internet et mobiles diffèrent à bien des égards, ils ont une chose en commun : une qualité de transmission relativement médiocre. Il est impossible de pouvoir évaluer avec fiabilité la latence du réseau et la perte de paquets, ainsi que leurs répercussions négatives sur les applications critiques.

En bref, les principales tendances dans l'évolution des réseaux d'entreprise sont : la réduction de la distance vers le data center de cloud ; les content delivery networks (CDN) ; et les technologies telles que l'accélération du trafic et les protocoles dynamiques de routage pour la distribution orientée application.

ACCÈS VIA DES PASSERELLES

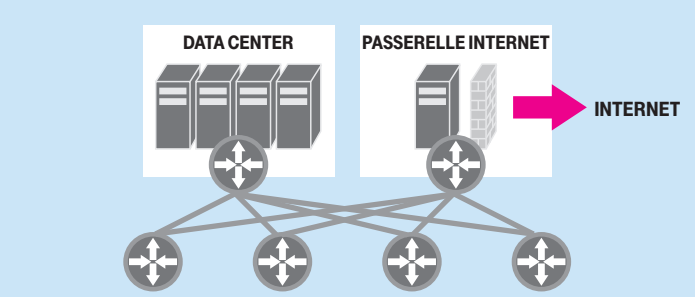


FIG. 8 : Conception en étoile des réseaux d'entreprise. Source : T-Systems

CLOUD PUBLIC SUR RÉSEAUX D'ENTREPRISE

Ces dernières années, le déploiement de stratégies de cloud hybride par les services informatiques a fréquemment été marqué par le phénomène du « shadow IT ». Ce terme décrit la souscription et l'utilisation de services de cloud public sur Internet sans l'approbation ou à l'insu du service informatique. Comme il existe une offre très diversifiée d'applications extrêmement flexibles et attractives, le phénomène continuera à se développer. Les DSI n'ont donc pas fini d'avoir mal à la tête. En effet, le cloud public est principalement prisé par les consommateurs, pour qui la sécurité n'est pas la priorité première (Figure 9). Mais pour les DSI, la sécurité est cruciale, compte tenu des impératifs juridiques et des risques économiques associés. Par ailleurs, à mesure qu'augmente le trafic sur Internet, la menace d'un goulot d'étranglement au point d'entrée des réseaux d'entreprise se précise en raison du nombre limité de passerelles utilisées par les architectures traditionnelles pour acheminer tous les flux de données vers le cloud public.

PRÉVISIONS EN TERMES D'ABONNEMENTS CLOUD PERSONNELS

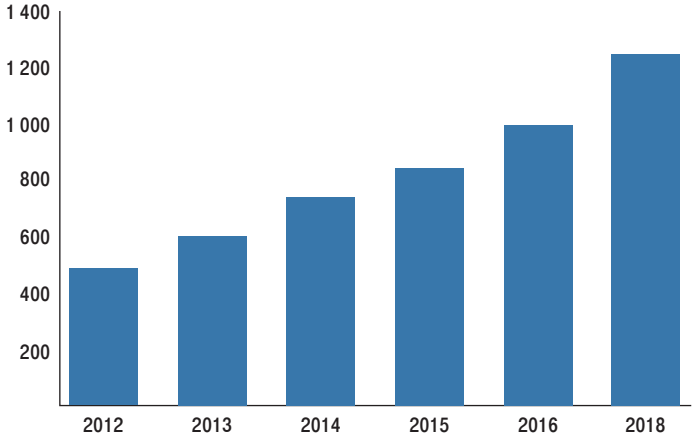


FIG. 9 : Projection du nombre d'abonnements souscrits par des utilisateurs finaux à un service cloud dans le monde (en millions). Source : IHS

AUGMENTATION DU TRAFIC VIA LES APPLICATIONS DE CLOUD PUBLIC

Une étude menée par Skyhigh suggère qu'en moyenne 80% du trafic réseau lié à des logiciels cloud est généré par seulement 15 applications. Ce chiffre inclut des applications autorisées dans le cadre professionnel et des logiciels utilisés à des fins professionnelles ou personnelles sans aucune approbation (Figure 10).

La Figure 11 indique d'ailleurs que le nombre total d'applications détectées sur les réseaux d'entreprise s'est envolé en un an seulement. Dans le cadre de cette étude, 13 millions d'employés de 350 entreprises ont été interrogés quant aux applications utilisées au travail.

Un autre résultat indique qu'en règle générale, la DSI n'est pas pleinement au courant des applications réellement utilisées, et révèle l'impact de chacune de ces applications sur les flux de données.

REPARTITION DU TRAFIC DE DONNÉES

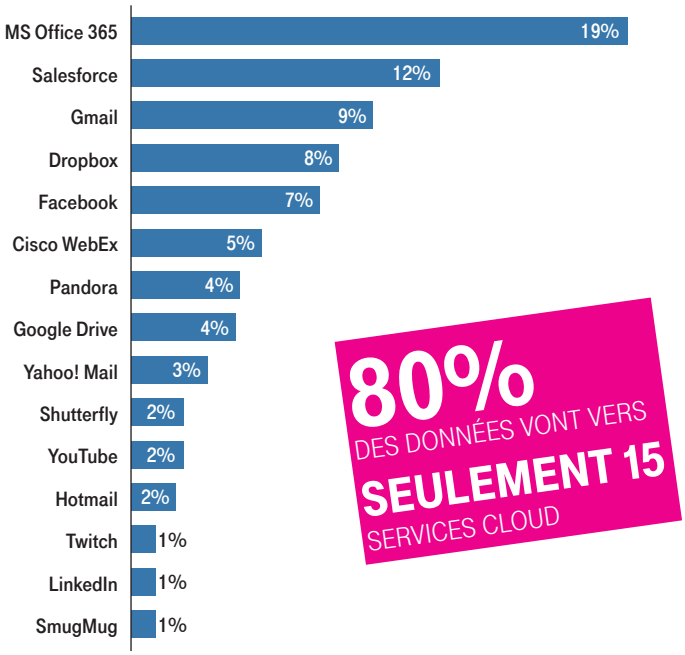


FIG. 10 : Trafic de données cloud par application. Source : Skyhigh Networks

RISQUES DE SÉCURITÉ

Malheureusement, il n'est pas possible d'empêcher purement et simplement l'utilisation de logiciels non autorisés à l'aide d'un pare-feu. La communication entre la majorité des applications dans le cloud et

ÉVOLUTION DU NOMBRE D'APPLICATIONS

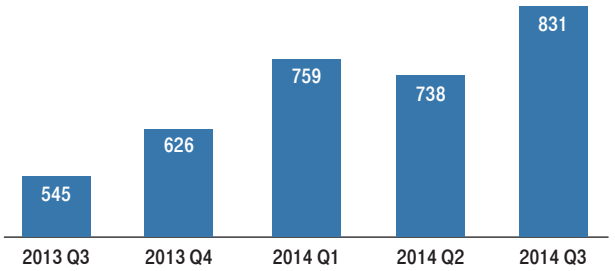


FIG. 11 : Nombre d'applications sur les réseaux d'entreprise. Source : Skyhigh Networks

les appareils des utilisateurs se fait aujourd'hui via HTTP ou sous forme chiffrée via le protocole HTTPS. Ces derniers étant les standards pour la transmission de contenu sur le Web, il est extrêmement difficile de faire la distinction entre les applications autorisées et non autorisées.

Par le passé, il était possible de filtrer ou de bloquer les applications de messagerie électronique ou encore de téléphonie sur IP, car leurs protocoles utilisaient des ports ou groupes de ports dédiés aux communications. Si une entreprise voulait désactiver le protocole POP3 pour la messagerie électronique externe par exemple, il lui suffisait de bloquer les ports 110 et 995.

Aujourd'hui, les utilisateurs de Google Mail ou d'Office 365 peuvent envoyer et recevoir des messages via leur navigateur web. Ces applications offrent les mêmes fonctionnalités puissantes qu'un client de messagerie électronique installé sur un ordinateur de bureau ou portable. Cependant, vu que l'application du navigateur utilise le protocole HTTPS pour communiquer avec le serveur, il est impossible de distinguer ce trafic chiffré de toute autre activité de navigation. Le seul moyen d'empêcher l'utilisation de Gmail est de bloquer l'URL correspondante. Mais l'utilisateur peut contourner cet obstacle facilement, puisque Gmail est accessible via plus de dix URL, différents serveurs proxy et l'environnement « Gmail lite ». Par conséquent, le blocage des accès est plus chronophage pour l'équipe de sécurité informatique. Gmail est une application populaire dont le fonctionnement et les fonctionnalités sont bien connus. Qu'en est-il des 830 autres produits (Figure 11) ? Par ailleurs, quelles nouvelles applications viendront s'ajouter à la liste à l'avenir ? Et que peut faire le service informatique si un utilisateur crée une connexion VPN SSL vers un serveur privé pour contourner les mécanismes de blocage ?

Les méthodes de filtrage et mécanismes de sécurité conventionnels ne permettent pas de faire la distinction entre les applications cloud autorisées ou non.

À l'heure actuelle, les systèmes de surveillance et de gestion des réseaux ont moins de visibilité et de contrôle sur le trafic de données, comme le montre la Figure 12. Des études menées auprès d'administrateurs et d'utilisateurs ont révélé que de nombreuses applications restaient utilisées alors que les services informatiques cherchaient à les bloquer. Même les salariés n'ayant pas de connaissances approfondies en informatique peuvent contourner relativement facilement les filtres d'un pare-feu. Des logiciels à risque peuvent donc traverser les barrières de sécurité des entreprises et accéder à des données sensibles. Comme le démontre l'étude de Skyhigh Networks, le vol de données ou de renseignements professionnels sensibles par des acteurs internes représente une menace majeure (Figure 13). En ne cherchant pas activement à bloquer les applications dans le cloud et en choisissant de les tolérer, les entreprises conservent au moins une certaine visibilité sur l'utilisation par leurs employés de services potentiellement préjudiciables (LiveLeak, par exemple).

ÉCART DE PERCEPTION DANS LA GESTION DU CLOUD

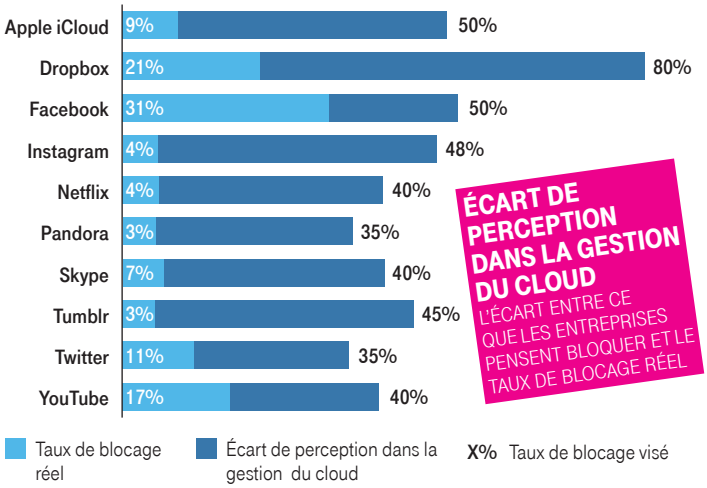


FIG. 12 : Taux de blocage d'applications réel et visé sur les réseaux d'entreprise. Source : Skyhigh Networks

INCIDENTS CAUSÉS PAR DES ACTEURS INTERNES

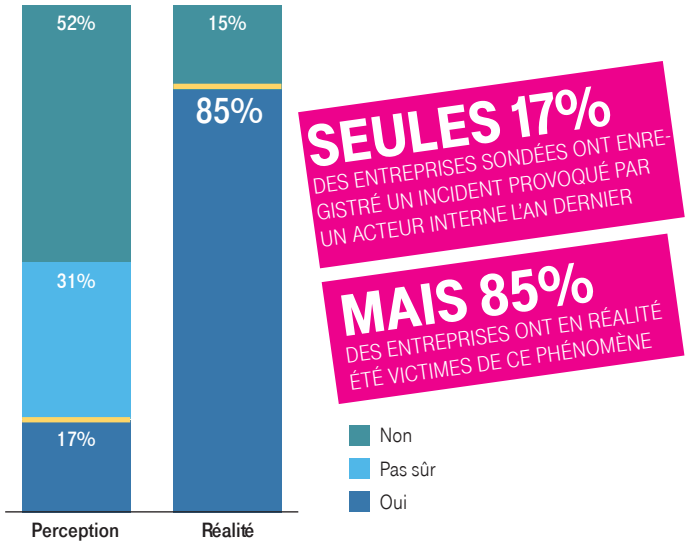


FIG. 13 : Menace perçue et incidents de sécurité réels imputables à des acteurs internes d'une entreprise. Source : Skyhigh Networks

Les tendances relatives à l'utilisation du cloud telles que :

- la croissance rapide de l'utilisation d'applications autorisées ou non dans des environnements de cloud public,
- la migration des données des postes de travail vers les data centers (avec Office 365 et Sharepoint, par exemple),
- la généralisation des protocoles HTTP et SSL, et
- la numérisation croissante des savoirs et des décisions rendent la question de la sécurité des données et de l'information essentielle pour les DSI.

Le marché de la sécurité connaît une croissance explosive, comme l'illustrent les historiques et prévisions de ventes de pare-feu d'entreprise récapitulés dans la Figure 14. Les fournisseurs de services réseau d'entreprise ont donc l'occasion de présenter la sécurité de leurs plates-formes privées sous un jour nouveau, mais également de se distinguer de la concurrence grâce à des offres intégrées.

PRÉVISIONS GLOBALES DU MARCHÉ DES PARE-FEUX D'ENTREPRISE PAR RÉGION

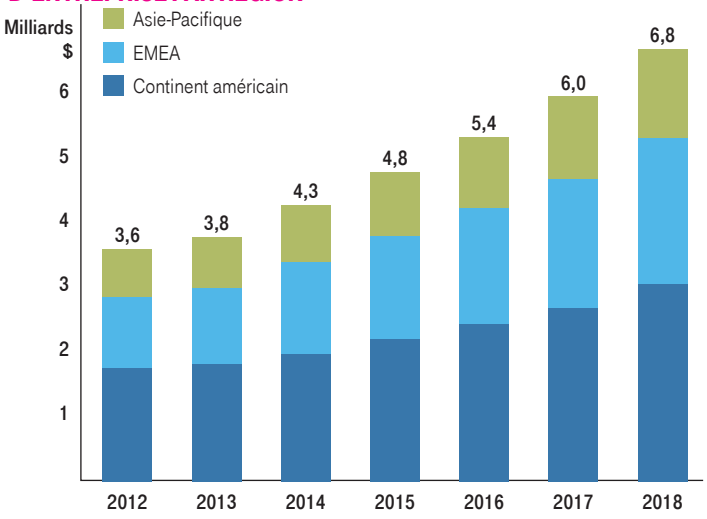


FIG. 14 : Évolution du marché mondial des pare-feu d'entreprise. Source : ASDReports

FLUX DE TRAFIC

Les réseaux d'entreprise sont traditionnellement dans une configuration en étoile (Figure 8). Les utilisateurs de chaque site accèdent à un data center centralisé au niveau régional ou mondial, qui est directement intégré au réseau via des liaisons à bande passante élevée et haute redondance. Ces data centers hébergent des applications critiques telles que SAP et des serveurs de messagerie. Tous les échanges concernant des données ou applications résidant dans un cloud public ont lieu via un nombre très limité de passerelles Internet, situées à des points stratégiques et protégées par un ou plusieurs pare-feux.
Le modèle en étoile était, par le passé, parfaitement adapté à la nature des applications d'entreprise. En effet, très peu d'entre elles avaient besoin d'un accès à Internet (tout au plus les messageries électroniques, les navigateurs et les serveurs web). Mais face aux exigences des logiciels actuels, cette approche montre des signes d'usure. L'explosion des volumes de données fait notamment apparaître deux défis majeurs :

1. L'augmentation sensible des besoins en bande passante au niveau des passerelles.
2. La dépendance de plus en plus forte des employés de bureau vis-à-vis de l'accès au réseau et de la passerelle Internet.

Il apparaît donc nécessaire de mettre en place de nouvelles structures et nouveaux mécanismes. Il ne s'agit pas d'augmenter la bande passante des passerelles. Les approches récentes montrent la nécessité de tenir également compte de la localisation des passerelles, de prendre en charge l'accélération du trafic, d'assurer un routage orienté application et d'augmenter le nombre de passerelles principales.

LE RÔLE PRÉDOMINANT D'INTERNET

Le réseau doit assurer un accès rapide et fiable à tous les logiciels critiques de l'entreprise. Comme la répartition des applications entre les data centers et environnements cloud évolue avec le temps, il deviendra de plus en plus important d'y intégrer des composants réseau basés sur Internet. L'emplacement et le nombre de passerelles Internet jouent un rôle crucial, notamment en ce qui concerne la connectivité en situation de mobilité (personnel itinérant, télétravailleurs et bureaux satellites) via des tunnels cryptés. Ce type d'accès a en effet pris une importance considérable récemment. Les employés en attendent des performances comparables à celles des postes de travail généralement reliés directement au réseau d'entreprise, c'est-à-dire des temps de réponse courts et un débit élevé. Sur les réseaux des grandes multinationales, ces critères peuvent être satisfaits au mieux en déployant un nombre de passerelles adéquat.

Le prix du trafic de données sur Internet ne cesse de chuter depuis des années, alors que la qualité des transmissions grimpe (Figure 15). Par conséquent, Internet est progressivement devenu une alternative à

ÉVOLUTION DU PRIX ET FIABILITÉ DES CONNEXIONS INTERNET 1998-2015

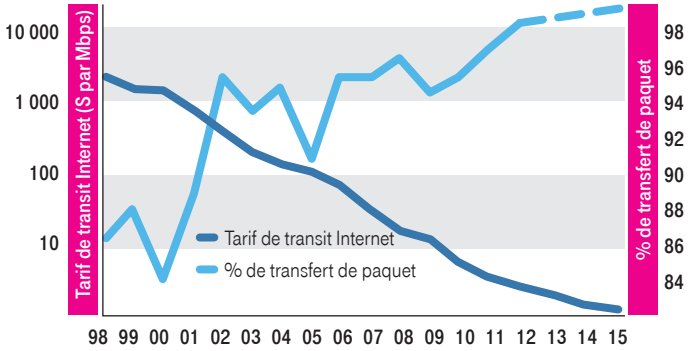


FIG. 15 : Évolution du prix et de la fiabilité des connexions Internet 1998-2015. Source : DrPeering.net

des plates-formes IP VPN privées (et coûteuses en comparaison). Les fournisseurs d'équipements tels que Cisco et Riverbed ont lancé des produits dont ils affirment qu'ils remplacent les réseaux MPLS par des réseaux purement basés sur Internet. Cette affirmation, justifiée ou non, fait l'objet d'une polémique féroce. Certains sont en faveur de réseaux overlay plus sûrs et aux performances supérieures basés sur des infrastructures hétérogènes (MPLS, Ethernet), avec une intégration flexible d'Internet. Les autres préfèrent des passerelles vocales centrales et des PBX centraux (VoIP sur WAN). Tout cela met en évidence les faiblesses persistantes d'Internet en tant que plate-forme d'entreprise (ainsi que son incapacité dans sa forme actuelle à remplacer totalement le MPLS).

L'ÉTAT DU MARCHÉ

Les frontières entre les technologies de l'information (IT) et les télécommunications (TC) se brouillent. Les fournisseurs et prestataires de services de ces deux segments étendent leurs offres de produits au territoire voisin. Dans leur quête de nouveaux clients, les startups utilisent des technologies innovantes, comme le software-defined networking (SDN) ou la virtualisation des fonctions réseau (NFV) dans le but de s'affirmer même sur le marché des réseaux d'entreprise internationaux. Toutefois, bien qu'il soit envisageable d'exploiter des segments de niche avec de nouveaux produits, le risque d'effectuer de lourds investissements sans aucun retour est également présent. Dans le même temps, les opérateurs risquent la perte de parts de marché s'ils ne parviennent pas à s'adapter au rythme effréné de l'innovation.

FOURNISSEURS PROPOSANT DES SERVICES CLOUD

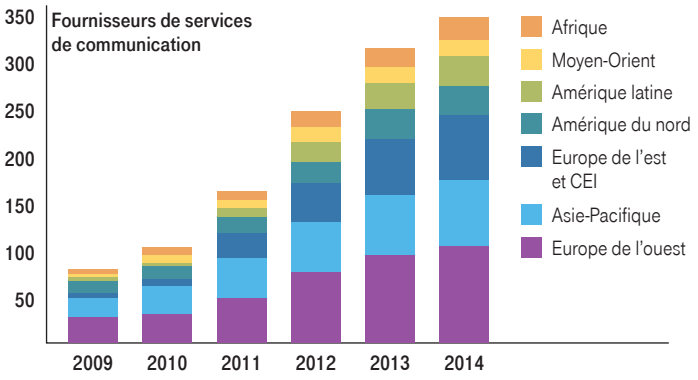


FIG. 16 : Nombre de fournisseurs de services de communication proposant des services cloud. Source : Ovum

LES FOURNISSEURS DE SERVICES MPLS TRADITIONNELS

Ces dernières années, les fournisseurs de services MPLS internationaux ont tous élargi leurs portefeuilles pour y inclure des services basés sur le cloud. Leur stratégie : amasser rapidement des ressources de calcul sur les nœuds réseau du monde entier, et fournir à leurs clients des services de cloud privé via leur infrastructure réseau existante (Figure 16).

Selon une étude d'Ovum, cette stratégie semble payante (Figure 17). Les recettes générées en associant services cloud et services réseaux augmentent de façon démesurée. Mais cela n'a pas forcément conduit à une augmentation des recettes globales pour les opérateurs de télécommunications, notamment parce que les nouveaux services cloud cannibalisent les produits existants.

Les opérateurs de réseaux d'entreprise sont ouverts à l'interfaçage avec les environnements cloud des grands acteurs internationaux, tels que Microsoft et Amazon. En développant ainsi leur portefeuille, ils peuvent proposer à leurs clients des services cloud couplés à la sécurité et à la qualité élevées d'une plate-forme de réseau privé. En outre, ils bénéficient de l'activité croissante et de recommandations de la part des principaux fournisseurs de services cloud.

Il est trop tôt pour dire si l'association de services cloud et réseaux sera déterminante sur le marché du WAN d'entreprise. Plusieurs fournisseurs mettent en œuvre des interfaces vers des plates-formes cloud et incorporent de plus en plus des services basés sur Internet dans leur portefeuille d'offres. Toutefois, leurs offres varient en termes de prise en charge des clouds privés et publics, de diversité géographique, de diversité de fournisseurs et de service client, ainsi qu'en fonction de leur capacité à proposer des connexions sécurisées (VPN) via une plate-forme de réseau privé.

Ils peuvent également se démarquer en intégrant des applications propriétaires (SaaS) à leurs portefeuilles de services réseaux. Par exemple, ils peuvent développer leurs portefeuilles afin d'y inclure des services de sécurité et de gestion du trafic (DDoS, scénarios de déchargement) et servir de nouveaux segments de marché.

La croissance dynamique du marché des services cloud contraint plus ou moins les fournisseurs de services réseau à intégrer des technologies

RECETTES LIÉES AU CLOUD

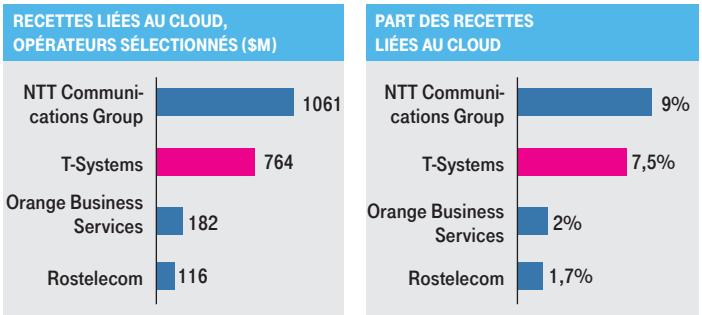


FIG. 17 : Prévisions des recettes issues de services cloud en 2013. Source : Ovum

orientées logiciel innovantes telles que le SDN et la NFV dans leurs programmes R&D. L'orientation future du marché des services réseau est de toute évidence fortement influencée par les évolutions dans le secteur de l'informatique, raison pour laquelle ces opérateurs de réseau devront fonctionner et penser comme des entreprises de services informatiques. S'ils ne négocient pas habilement ce virage structurel, ils en resteront à fournir des services d'infrastructure sur le marché du réseau hybride d'entreprise et seront confrontés à une vive concurrence et à la pression des coûts.

FOURNISSEURS DE SERVICES INFORMATIQUES TRADITIONNELS

La frontière entre IT et télécommunications est de plus en plus floue. Les réseaux de télécommunications ne peuvent pas fonctionner sans logiciels. Les routeurs et autres composantes du réseau deviennent des ordinateurs hautes performances, ouvrant la voie à la virtualisation des fonctions réseau (NFV). Chaque fonction peut ainsi être encapsulée et transférée du routeur vers des data centers. Les pare-feux en sont un bon exemple. Ces solutions incluent souvent plusieurs composantes logicielles qui assurent la sécurité des données et des informations, de la couche Ethernet aux mécanismes antivirus.

Les fournisseurs de services informatiques sont actifs depuis longtemps sur le marché des télécommunications, bien qu'ils aient principalement tenu un rôle de fournisseurs de composantes plutôt que de fournisseurs de réseaux d'entreprise. Le marché de l'IPSec et des VPN SSL, pour les particuliers et les petites entreprises, est une exception. Dans ce secteur, des fournisseurs de logiciels tels que CactusVPN, Mullvad, et NordVPN règnent en maîtres et les ventes ont principalement lieu sur Internet et les app stores de Google et Apple. À l'inverse, les moyennes et grandes entreprises restent la chasse gardée des opérateurs de télécommunications traditionnels tels que Deutsche Telekom/T-Systems, Orange, NTT, BT et AT&T. Cela s'explique principalement par les énormes dépenses d'investissement consenties au niveau des infrastructures réseau, et par la réduction des marges bénéficiaires. Ces éléments combinés créent une barrière à l'entrée considérable sur ce marché. Cette corrélation se reflète dans les classements des analystes, qui se basent en partie sur le nombre de nœuds des dorsales. Autre critère : le fait d'exploiter ou non

TAILLE DU MARCHÉ MONDIAL DU SDN ET PRÉVISIONS, 2012 - 2018 ($M)

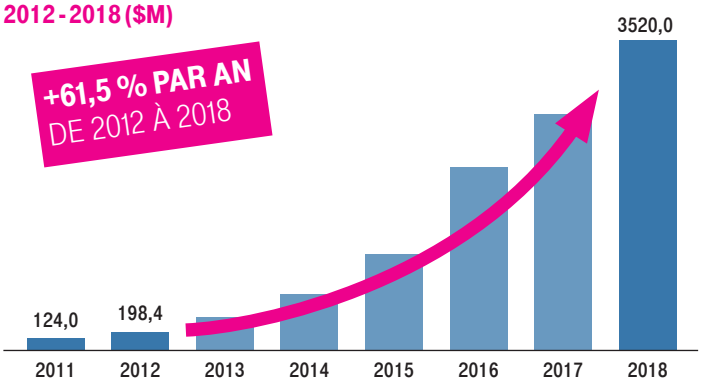


FIG. 18 : Prévisions de croissance du marché du software-defined network 2012-2018
Source : Transparency Market

son propre réseau. Ceci étant dit, les logiciels sont sur le point de changer la donne et l'on peut prévoir que ces critères de classement auront moins d'importance d'ici quelques années.

Nombreux sont les éditeurs et les startups compétents en matière de télécommunications à développer actuellement des produits et parfois des portefeuilles entiers de services réseaux basés sur le SDN et la NFV. Avec le SDN, contrairement au MPLS, les couches de contrôle et d'acheminement sont séparées. Les composants d'acheminement continuent à être mis en œuvre sur les nœuds (par exemple les routeurs et les commutateurs), alors que les éléments de contrôle sont centralisés et exploitent des API. Cela permet d'utiliser du matériel standardisé (tel que des serveurs x86)sur les nœuds, tandis que les éléments de contrôle sont virtualisés dans des data centers. Par conséquent, le SDN réduit les coûts matériels et d'exploitation des réseaux. En théorie, les frameworks

LES DATA CENTERS CLOUD DONNENT LE TON POUR LES INVESTISSEMENTS DANS LES SDN

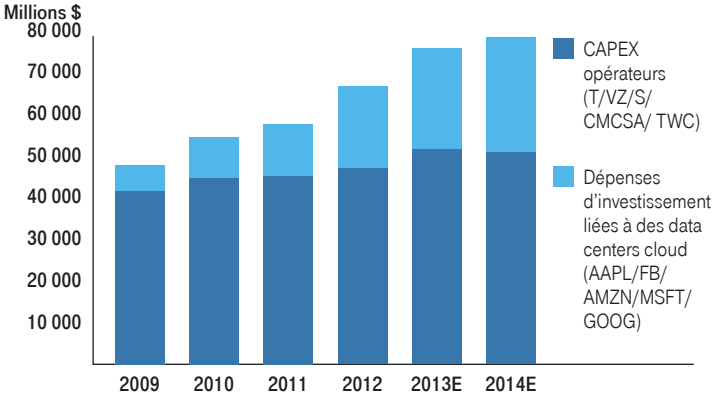


FIG. 19 : Dépenses d'investissement dans le SDN de la part des cinq plus importants fournisseurs de services cloud et fournisseurs de services traditionnels (USA).
Source : Goldman Sachs

open source tels qu'OpenFlow permettent l'interopération de différentes composantes réseau entre les plates-formes de différents fournisseurs. Encore faut-il tester ce modèle dans son intégralité afin d'en connaître l'efficacité dans le monde réel, car le marché du SDN est encore très jeune (Figure 18). Un bon exemple de plate-forme réseau innovante est la Next Generation Enterprise Alliance (ngena) fondée par Deutsche Telekom/T-Systems, Reliance et SK Telecom afin de lancer en 2017 un portefeuille de services entièrement basés sur le SDN.

L'objectif du développement de composants et de la mise en œuvre du SDN porte initialement sur les data centers (Figure 19). Ces dernières années, cependant, les fournisseurs de réseaux d'entreprise ont investi dans la R&D autour de cette technologie, et des startups telles que ngena ont lancé avec succès des plates-formes réseau et des portefeuilles de services basés sur les technologies du SDN et de la NFV. Le déploiement du SDN au sein de réseaux WAN présente d'importants avantages, comme de réduire les coûts d'exploitation et de matériel. En outre, cette approche offre davantage de flexibilité en termes d'extensibilité et d'évolutivité.

Si ce modèle venait à gagner du terrain, le marché des réseaux de télécommunication changerait de manière considérable au cours des dix prochaines années. Tout dépendra des risques technologiques et du coût de lancement de telles plates-formes réseau au profit des grandes multinationales. L'introduction de ce modèle ne requiert pas seulement le remplacement de la majorité des composantes des plates-formes réseau. Des modifications importantes au niveau des processus opérationnels et donc structurelles s'imposent également. De nombreuses plates-formes SDN seront probablement développées parallèlement à des infrastructures existantes du fait des différences notables entre les technologies traditionnelles et récentes. Cela réduira l'avantage qu'ont les opérateurs sur les nouveaux arrivants, bouleversant ainsi la situation concurrentielle. Ils peuvent également continuer à exploiter leur infrastructure existante comme base d'une nouvelle plate-forme SDN, avant de migrer progressivement leurs services. Dans ce scénario, le réseau physique sera utilisé comme partie d'une infrastructure générique jusqu'à ce que son remplacement par un nouveau type de réseau soit intéressant d'un point de vue économique. C'est ce qui s'est produit quand le frame relay (FR) et l'ATM ont été supplantés par les systèmes IP MPLS (ces deux technologies d'ancienne génération continuant à occuper un rôle de niche dans l'accès au réseau).

FOURNISSEURS DE MATÉRIEL

La croissance rapide du cloud computing touche aussi les fournisseurs de matériel et de logiciels réseau. Les data centers doivent répondre à des normes extrêmement élevées en termes d'évolutivité et de disponibilité, ce qui pose de nouveaux défis pour les infrastructures réseau. Dans ce contexte, à l'avenir, les réseaux devront :

- assurer une bande passante très élevée,
- distribuer les charges de travail intelligemment,
- synchroniser les données entre data centers principaux et de secours,
- ajouter rapidement des capacités de calcul et de stockage pour satisfaire la demande.

ÉVOLUTION DU MARCHÉ DE LA CONSTRUCTION DE DATA CENTERS (MILLIARDS $)

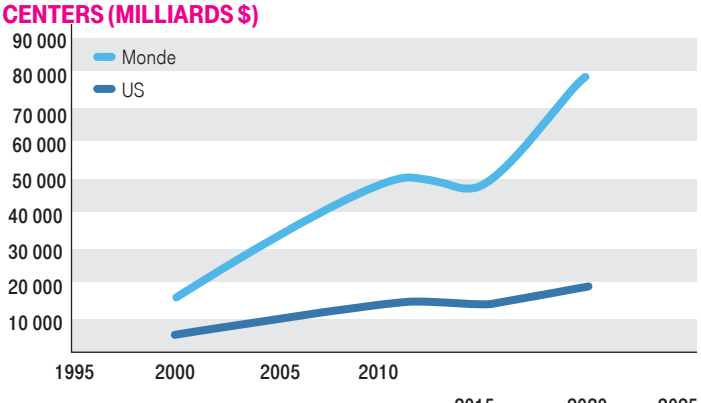


FIG. 20 : Évolution du marché mondial de la construction de data centers (en milliards de $ US). Source : datacenterpro.wordpress.com

Le nombre croissant de data centers dans le monde (Figure 20) contribuera également à affecter le marché des équipements et logiciels réseau :

- La croissance globale enregistrée sera principalement liée à la progression de la demande en infrastructures de data center.
- La stratégie des principaux fournisseurs sera axée sur le développement de nouveaux matériels et logiciels pour le SDN et la NFV.

MARCHÉ DES INFRASTRUCTURES RÉSEAU

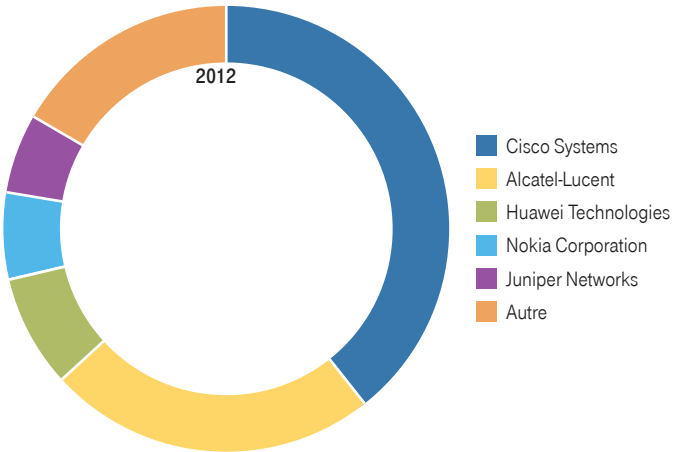


FIG. 21 : Marché mondial des infrastructures réseau.
Source : pcsemicon.blogspot.com

Les fournisseurs d'infrastructure réseau (Figure 21) participent activement à ces tendances. Ils augmentent leurs budgets de R&D afin d'être compétitifs et d'obtenir leur part du marché de la NFV et du SDN. Cette première technologie a été créée comme une base pour les réseaux déployés dans des data centers ;elle a ensuite évolué pour devenir un élément essentiel de la base technologique des réseaux WAN de nouvelle génération. Elle établit un pont entre les marchés des data centers et l'infrastructure WAN, et offre une solution permettant aux acteurs d'un de ces deux marchés de s'implanter dans l'autre. Cisco tire déjà parti de cette opportunité en investissant lourdement dans le SDN et la NFV pour accroître sa part sur le marché des infrastructures. La situation concurrentielle sur le marché du WAN devrait également être affectée par ces nouvelles technologies. Une tendance claire se dessine : les fournisseurs se désintéressent désormais des équipements spécialisés et leur préfèrent des capacités de modélisation logicielle de leurs fonctions. Ces logiciels peuvent être installés sur du matériel générique et dans des data centers. Ainsi, à l'avenir, les opérateurs réseau auront le choix de remplacer certaines de leurs dépenses d'investissement par des dépenses d'exploitation.

Les fournisseurs d'infrastructures sont face à des défis quelque peu différents. Ils doivent étendre leurs portefeuilles et exploiter de nouveaux marchés pour réaliser des marges supérieures et contrer les effets de la chute des prix du matériel. S'ils ne peuvent pas se permettre les investissements nécessaires, leur part de marché diminuera à mesure que le marché continuera à se consolider.

STARTUPS

La croissance rapide du cloud computing va de pair avec la complexité accrue des réseaux de data centers. Comme l'adoption de la virtualisation s'accélère, il en va de même pour la distribution dynamique des processus de calcul et de stockage au sein et entre les data centers. Les performances de ces derniers dépendent donc largement de la capacité du réseau.

Un certain nombre de jeunes entreprises ont cherché à profiter de cette tendance et ont développé divers produits relatifs au SDN pour des réseaux LAN. Et la demande en réseaux haute performance dans les data centers n'est pas le seul facteur qui rende le climat favorable aux startups. Les principaux fournisseurs de composants réseau, tels que Cisco, doivent ajouter de nouveaux produits à leur portefeuille pour survivre et prospérer dans cet environnement dynamique. Nombre de ces nouveaux venus se sont lancés dans l'intention d'être rachetés. Cette tactique attire les sociétés de capital-risque, qui apportent le financement supplémentaire. Selon IDC, les composantes du SDN totalisent déjà 8,7% du marché du WAN, une part qui ne fait que croître. Les startups investies dans le SDN ont reçu environ 650 millions de dollars US ces dernières années de la part de sociétés de capital risque. Les analystes estiment que cette somme devrait doubler dans les trois prochaines années.

Outre ngena, Aryaka fait partie des jeunes pousses les plus reconnues du secteur du SDN et est axée sur les réseaux étendus. Elle bénéficie d'une vaste expérience en matière d'optimisation de WAN, et explore désormais cette technologie conjointement avec le SDN pour offrir un service de réseau étendu Ethernet et Internet à l'échelle mondiale. En mars 2015, la société avait déjà acquis au total 97,2 millions de dollars

US de la part de fonds de capital-risque. Viptela, quant à elle, combine SDN et réseau hybride. Elle prend en charge le MPLS, Ethernet et Internet avec un équipement dédié, et possède le potentiel nécessaire pour travailler main dans la main avec des fournisseurs établis de services réseau internationaux . Une société de capital-risque a apporté au nouveau venu un financement initial de 33,5 millions de dollars US en 2014.

La part du marché du SDN au sein des réseaux d'entreprise gérés par des fournisseurs de WAN reste faible. Elle tourne actuellement autour de 15 à 18 %, et équivaut à un peu plus de 1% du marché des réseaux étendus. Les spécialistes du marché se focalisent sur la prise en charge de vastes réseaux comprenant des centaines ou des milliers de sites, comme par exemple pour des agences bancaires. En effet, les économies de coûts liées au surplus d'efficacité du SDN sont supérieures à l'investissement nécessaire pour acquérir des logiciels complexes et développer une expertise et des processus au sein de l'organisation. Toutefois, en ce qui concerne le marché des réseaux d'entreprise dans son ensemble, aucun changement d'envergure n'est prévu pour les trois prochaines années.

Les fournisseurs de WAN traditionnels doivent profiter au maximum de cette « période de grâce » afin de s'assurer une part de ce marché émergent à l'avenir. Ils doivent gagner en expertise en matière de SDN et proposer de nouveaux produits. À court terme, ils peuvent développer de nouveaux marchés de niche pour leur architecture SDN pour compenser les baisses de recettes et de profits liées au MPLS. À long terme, le SDN devrait devenir la principale technologie des principaux grands fournisseurs de services réseau. Mais les portefeuilles de services basés sur la technologie MPLS, comme IntraSelect de T-Systems, continueront à jouer un rôle important dans les réseaux d'entreprise, et à être déployés sur les dorsales.

LE CLIENT

Le rôle du DSI évolue. Il est évident que l'importance de l'IT et des télécommunications dans la chaîne de valeur continue de croître. Traditionnellement, les DSI basaient leurs décisions sur une analyse du retour sur investissement (là où les coûts de l'infrastructure sont de première importance). Aujourd'hui, ils ressentent toujours cette pression concernant les coûts, mais doivent en même temps prendre en charge l'internationalisation des entreprises par le biais de services informatiques et réseau. Cela passe par :

- De nouvelles capacités d'analyse de données (en utilisant, par exemple, des technologies de traitement des big data)
- Des offres personnalisées à chaque contexte client
- Une meilleure expérience client
- De nouveaux modèles économiques grâce à la numérisation
- Une évolutivité et une élasticité plus importantes au niveau des ressources
- Des produits et processus de plus en plus connectés (IdO/quatrième révolution industrielle)

Les services IT et réseau deviennent les éléments clefs de l'innovation. Les décisions relatives à l'infrastructure jouent un rôle essentiel dans la réussite économique. Et, à leur tour, les demandes relatives aux WAN évoluent.

Le coût des réseaux d'entreprise reste un des principaux facteurs influençant les décisions d'achat, mais la capacité d'innovation prend de l'importance. Dans l'ensemble, la question centrale est la suivante : en quoi l'offre du fournisseur de services contribue-t-elle à la réussite économique ? À l'heure actuelle, il est possible de trouver des réponses plus larges et nuancées à cette question.

LES FOURNISSEURS DE CLOUD ET LEURS SERVICES

En termes simples, les services cloud sont une combinaison de puissance de calcul, de stockage et de logiciels dans des data centers. Contrairement à un hébergement traditionnel, ces services sont mis en oeuvre sur une infrastructure virtuelle et entièrement automatisée. Les utilisateurs bénéficient ainsi de coûts moins importants, de délais de transmission accélérés et des ressources très flexibles. Les nouveaux venus sur le marché des logiciels ont contribué à alimenter la croissance du marché des services cloud. Certaines solutions ont ainsi d'abord connu un succès auprès des particuliers, puis des entreprises (Figure 22). Dropbox est d'ailleurs l'illustration parfaite de cette évolution.

ÉVOLUTION DU MARCHÉ DU CLOUD

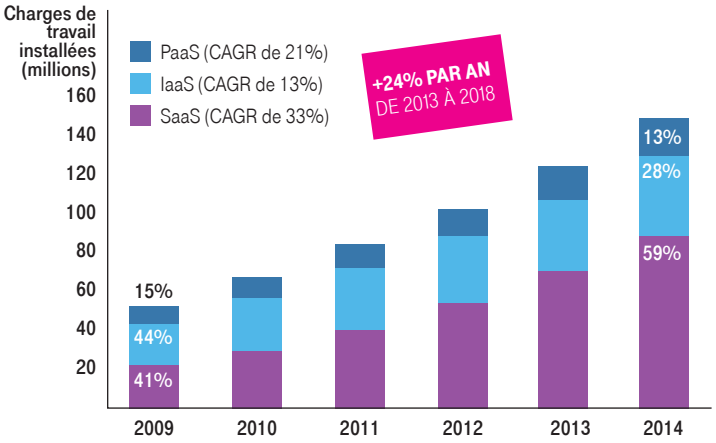


FIG. 22 : Évolution des marchés du SaaS, de l'IaaS et du PaaS. Source : Cisco

Les services cloud peuvent être divisés en trois catégories. L'IaaS, qui offre une puissance de calcul virtuelle dans le cloud. Du point de vue de l'utilisateur, cela équivaut à avoir un CPU, de la RAM et de la ROM sans système d'exploitation. Le PaaS fait référence aux machines virtuelles, systèmes d'exploitation inclus. Et le SaaS, qui fournit des applications standardisées fournies depuis le cloud, en général de manière totale-

MARCHÉ DES INFRASTRUCTURES ET PLATES-FORMES CLOUD (MILLIARDS DE $, 2013-2018)

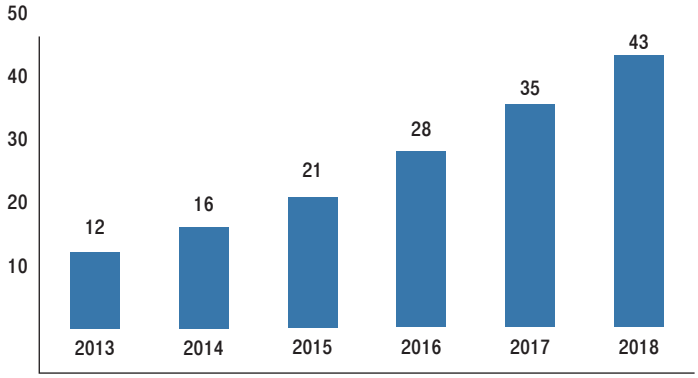
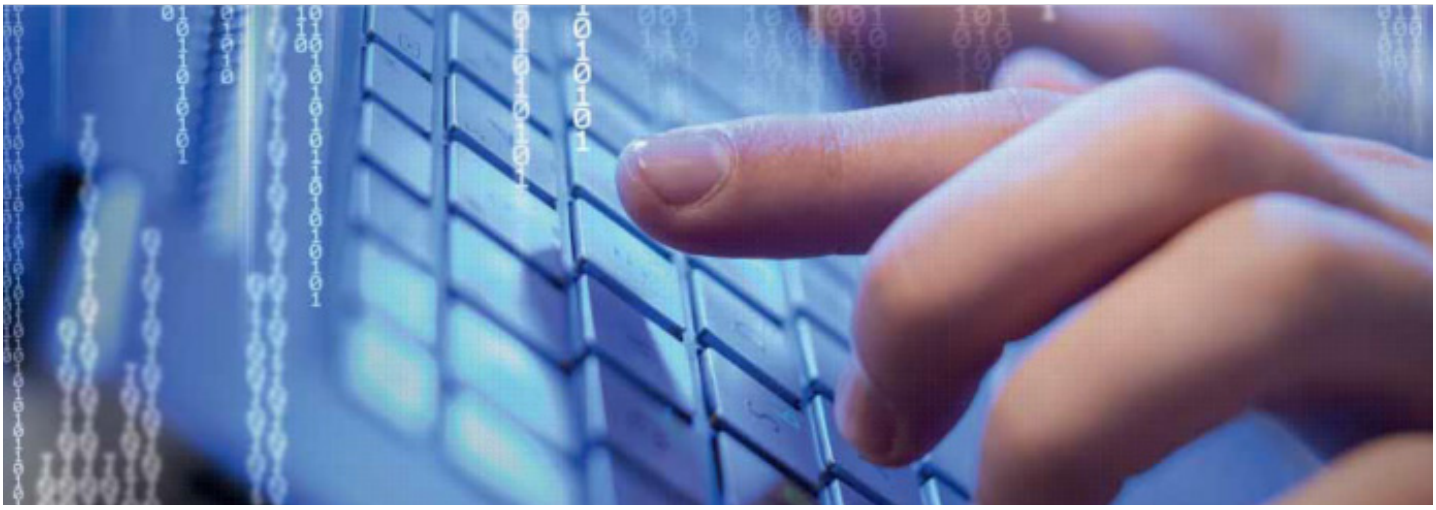


FIG. 23 : Évolution du marché du cloud selon les analystes. Source : STL Partners



ment automatisée (par exemple, Dropbox ou Microsoft Office 365)

Le nombre de fournisseurs de IaaS et de PaaS est en augmentation tout comme la pression concurrentielle (Figures 23 et 24). Les services de base étant de plus en plus normalisés, les utilisateurs ont donc virtuellement plus de mal à les distinguer. Les clients ont déjà la possibilité de se procurer de la puissance de calcul depuis plusieurs sites afin de créer un environnement évolutif et doté d'une haute disponibilité.

CONCURRENCE SUR LE MARCHÉ DES SERVICES D'INFRASTRUCTURE CLOUD 3E TRIMESTRE 2014

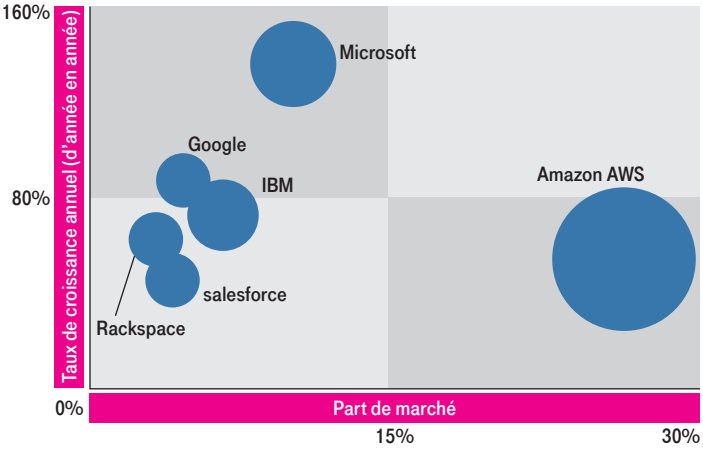


FIG. 24 : Situation concurrentielle sur le marché des services d'infrastructure cloud. Source : Synergy Research Group

Le principal fournisseur d'IaaS sur le marché mondial est de loin Amazon : selon le Magic Quadrant 2015 de Gartner, le marché continue à se consolider autour du fournisseur et de son premier concurrent éloigné, Microsoft. Cette consolidation a conduit certains fournisseurs d'IaaS à se retirer du marché. Par exemple, HP a décidé de mettre fin à son offre de cloud public HP Helion en janvier 2016. D'autres fournisseurs ont choisi de concentrer leurs efforts en matière d'IaaS sur des marchés de niche comme le cloud privé ou en exploitant des avantages politico-geéographiques. En octobre 2015, par exemple, Deutsche Telekom a annoncé le lancement de son offre IaaS dans le cloud public, « Open Telekom Cloud », résultat d'un partenariat avec Huawei. Open Telekom Cloud répond notamment aux inquiétudes du marché quant à la fin de l'accord « Safe Harbor ». L' invalidation de ce dernier signifie que la confidentialité des données de nombreuses organisations dépend désormais de l'emplacement du data center. D'où l'importance de recourir à un cloud hébergé et opéré en Europe.

Actuellement, une grande partie du marché de l'IaaS est dominée par quelques acteurs (Figure 24). Les fournisseurs de services réseaux ont moins d'interfaces à proposer vers des fournisseurs de cloud externes (ce qui facilite leur intégration à leurs portefeuilles). Selon l'étude « Cloud Connectivity Services in Europe » publiée en mai 2015 par IDC,

MARCHÉ DU PAAS MONDIAL PAR RÉGION, 2013, MILLIONS USD

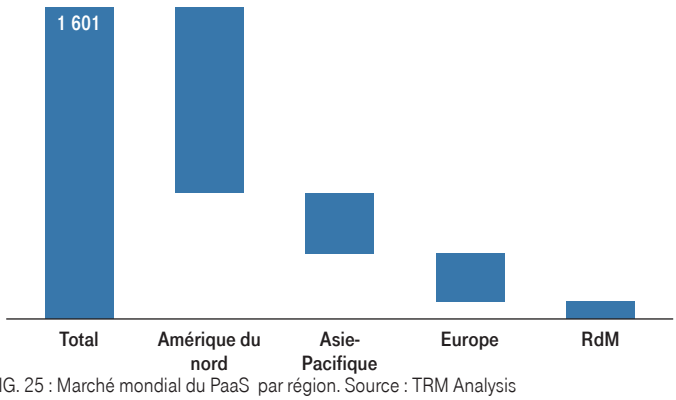


FIG. 25 : Marché mondial du PaaS par région. Source : TRM Analysis

la plupart des fournisseurs de services réseau dans le monde sont en interconnexion directe avec seulement quatre fournisseurs de services cloud : Amazon, Microsoft, Google et HP. Il existe également des connexions à d'autres clouds, mais qui varient selon les fournisseurs de services réseaux.

Géographiquement, en revanche, le marché du cloud est beaucoup plus varié. L'exemple parfait est celui du PaaS, un segment dominé par l'Amérique du Nord, suivie de l'Asie et de l'Europe (Figure 25). Logique, puisque les plus importants fournisseurs par la taille sont établis aux États-Unis. Toutefois, les marchés européen et asiatique ont connu une croissance importante ces dernières années et sont parvenus à gagner pas mal de terrain. Les analystes s'attendent à ce que cette croissance rapide se poursuive. L'Asie n'a pas seulement été le troisième marché de plus important en matière de services cloud en 2015, elle devrait aussi croître plus vite que l'Europe et lui subtiliser sa deuxième place.

TECHNOLOGIES RÉSEAU

Les réseaux d'entreprise n'ont pas beaucoup évolué depuis l'introduction du MPLS pour la transmission de données sur les WAN il y a 15 ans (à l'exception du remplacement de l'ATM et du frame relay par l'IP). Aucune nouvelle architecture n'a émergé pour remplacer ce protocole comme base des échanges de données sur les réseaux d'entreprise hébergeant des applications critiques. La baisse constante du coût des transmissions sur Internet a conduit la plupart des acteurs du marché à se tourner vers cette solution. Toutefois, la qualité du transfert de données sur Internet reste inférieure aux normes B2B en matière de sécurité, de latence ou de SLA. Par conséquent, les services réseaux basés sur MPLS tels que ceux proposés par Orange Business Services, BT, AT&T ou T-Systems, resteront dominants dans un avenir proche, en dépit de leur coût relativement élevé.

DÉCHARGEMENT DU TRAFIC

Ces dernières années, l'augmentation de la demande en bande passante a conduit à l'expansion mondiale de l'infrastructure Ethernet (Figure 26). Pour obtenir des bande passantes supérieures à 50 Mbps sur des WAN, cette technologie est souvent moins onéreuse que le MPLS. Toutefois, les économies relatives par Mbps ne suffisent pas à compenser les coûts engagés pour satisfaire la demande croissante en bande passante. C'est ce qui a conduit à l'introduction de modèles hybrides, où une part croissante des communications sur les réseaux d'entreprise est acheminée sur Internet à l'aide de mécanismes de tunnels sécurisés. La nature du trafic de données sur Internet rend la communication généralement moins coûteuse que sur des plates-formes de réseau privé telles que le MPLS ou l'Ethernet.

TENDANCES MONDIALES EN MATIÈRE DE BANDE PASSANTE EN ENTREPRISE

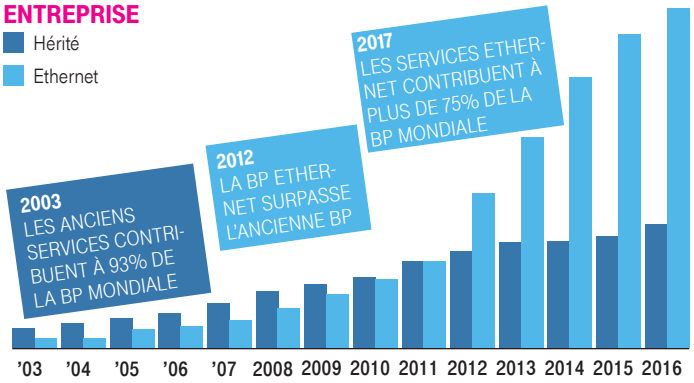


FIG. 26 : Croissance de l'Ethernet sur le marché mondial des infrastructures WAN. Source : verticalsystems.com

Exploiter Internet comme base de VPN requiert un routage intelligent des flux de données. Les applications sensibles à la latence (voix ou vidéo) ou la sécurité continuent à être prises en charge par MPLS. En revanche, les données destinées à des applications moins sensibles, comme la messagerie électronique, peuvent être transférées via des connexions Internet cryptées. Le déchargement du trafic permet d'effectuer un acheminement sur le réseau sur la base d'exigences de qualité de service. Son utilisation s'est généralisée pour optimiser les communications sur les réseaux d'entreprise terrestres ainsi que sur les réseaux mobiles pendant quelques années. Dans les deux cas, les flux de données non critiques ou non sensibles aux délais précédemment acheminés sur le réseau principal relativement coûteux sont basculés vers une plate-forme plus abordable. Cette approche réduit les coûts de bande passante ou, du moins, les maintient à un niveau constant en dépit du déploiement d'applications de plus en plus gourmandes telles que la communication vidéo ou les logiciels de stockage dans le cloud (Dropbox ou Microsoft SharePoint).

ROUTAGE EN FONCTION DES PERFORMANCES

Le routage basé sur les performances est susceptible de résoudre le problème de complexité associé au déchargement du trafic, et étend le concept à l'optimisation des performances réseau, et pourrait, du point de vue de l'utilisateur, à ce concept. Comme pour le déchargement du trafic, deux liaisons réseau sont activées depuis la succursale : l'une vers Internet et l'autre vers la plate-forme de réseau privé haute performance (en général Ethernet ou MPLS). Une instance de routage entre l'agence et le WAN sélectionne le meilleur parcours de transmission des données pour chaque application. Elle s'appuie pour cela sur des connaissances mises à jour de manière dynamique relatives à la performance de ce chemin réseau , et tient également compte des différentes exigences des applications. Contrairement au déchargement du trafic, où toutes les transmissions finissent par converger quelque part sur la plate-forme de réseau privé, sur les réseaux où le routage basé sur les performances est activé, il est également possible de joindre directement la destination via Internet. Cela peut être le cas quand une application externe, par exemple dans un data center de cloud public, doit être jointe via Internet. Le trafic de données destiné aux clouds publics peut ainsi être déchargé directement vers Internet sur le routeur de la succursale. Cette configuration offre deux avantages :

1. Seul le trafic minimum (critique) traverse le réseau privé principal, réduisant encore le coût en bande passante.
2. Les applications de cloud public peuvent être jointes directement depuis chaque site sans avoir à passer par une passerelle Internet distante quelque part sur la plate-forme de réseau privé.

RÉSEAUX OVERLAY

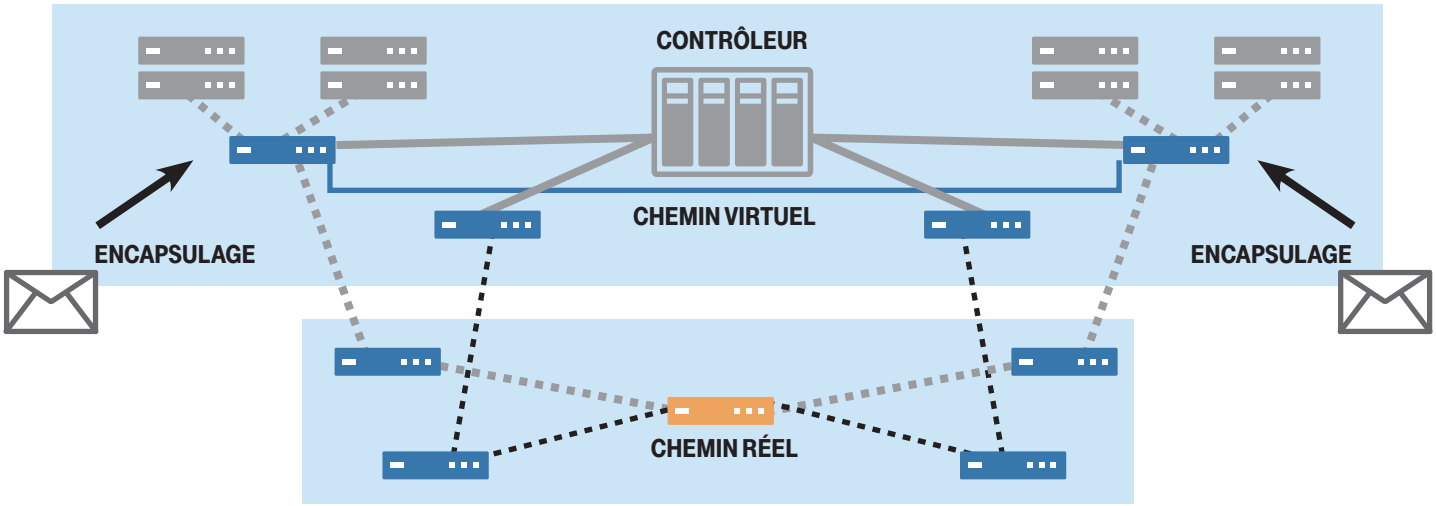


FIG. 27 : Le principe d'un réseau overlay. Source : Deutsche Telekom

L'inconvénient de cette technologie est que l'opérateur doit renoncer à un certain contrôle sur le routage du trafic sur le réseau, ce qui complique non seulement le suivi des problèmes de performance, mais rend aussi difficile, voire impossible, de proposer des SLA identiques à ceux des réseaux MPLS traditionnels.
Le routage basé sur les performances, et notamment la façon dont il est mis en oeuvre, dépendent du fournisseur d'équipements choisi (en général Cisco ou Riverbed)..

RÉSEAUX OVERLAY

Le principal défi lors de la mise en œuvre du routage basé sur les performances est d'assurer une protection du trafic entre plusieurs plates-formes à différents niveaux. Les réseaux overlay proposent une solution : ces réseaux privés virtuels sont généralement basés sur des tunnels IPSec ou GRE qui se superposent sur une ou plusieurs plates-formes réseau (par exemple, Internet et MPLS), en tenant compte des relations de communications au sein du réseau d'entreprise. Ils contrôlent le trafic indépendamment des plates-formes sous-jacentes (voir Figure 27). Tout cela contribue en théorie à rendre le réseau d'entreprise homogène et fluide en apparence, même dans une infrastructure hétérogène. L'organisation peut également s'occuper de son approvisionnement en infrastructure de façon dynamique à mesure que son réseau évolue. Toutefois, au niveau technique et opérationnel, il existe des dépendances entre l'infrastructure réseau et le réseau overlay, ce qui peut rendre l'exploitation plus difficile que prévu. Associé à la dernière génération de systèmes de gestion réseau, l'overlay devrait constituer un moyen rentable et convivial de configurer un réseau de manière dynamique.

VIRTUALISATION DU RÉSEAU ÉTENDU (WAN)

La virtualisation du WAN combine déchargement du trafic, routage basé sur les performances et réseaux overlay. En d'autres termes, des connexions réseau basées sur différentes plates-formes (MPLS, Ethernet, Internet, par exemple) sont associées pour créer un environnement réseau d'entreprise (Figure 28). La virtualisation permet à chaque site d'une entreprise de déployer des liaisons et des services réseau adaptés (tels que des pare-feux, des routeurs et des commutateurs). Le système rassemble alors toutes les connexions réseau de ce site pour former une connexion virtuelle unique avec une bande passante élevée et des paramètres de qualité de service différenciés. Par ailleurs, la virtualisation du WAN utilise également des mécanismes d'ingénierie du trafic dynamiques dans le but :

- de mieux utiliser les capacités réseau disponibles ;
- d'ajuster les vitesses de transfert en fonction de la sensibilité des applications ;
- de créer une redondance.

Un logiciel de contrôle intelligent et centralisé permet de gérer avec souplesse ces réseaux virtuels - par exemple, pour prendre en charge plusieurs applications avec des charges fluctuantes ; ou pour assurer une gestion efficace des modifications suite au déploiement de nouvelles composantes réseau ou de nouvelles politiques de sécurité.

VIRTUALISATION DES FONCTIONS RÉSEAU

Un autre moyen de réduire les coûts d'exploitation du WAN est de virtualiser des fonctions réseau habituellement intégrées à des routeurs ou des commutateurs. Ce matériel bien trop coûteux peut être remplacé par des serveurs x86 standard, ce qui peut avoir un effet significatif sur les dépenses d'investissement (CAPEX) dans de vastes systèmes réseau. La virtualisation des fonctions réseau (NFV) permet d'assurer une gestion centralisée des modifications réseau via des mises à jour logicielles, réduisant ainsi sensiblement les efforts nécessaires. Le déchargement du trafic, par exemple, requiert une surveillance décentralisée de tous les canaux disponibles, un routage décentralisé intelligent (en fonction des applications et des politiques) et un moteur de politique central. Ensemble, ces fonctions peuvent être optimisées grâce à une virtualisation de bout en bout. En outre, le point de contrôle central et l'utilisation de matériel abordable garantissent une certaine rentabilité. Un grand nombre de fournisseurs de matériel et de startups explorent actuellement cette approche. Toutefois, la technologie est toujours en développement et un modèle standard doit encore émerger. En attendant, les fabricants comme Cisco et Juniper offrent des équipements réseau basés sur la NFV (des routeurs, par exemple) associés à leurs propres plates-formes de calcul propriétaires. Il faut s'attendre à ce que de telles plates-formes existent pendant une période de transition relativement courte à l'issue de laquelle une norme haute performance faisant l'unanimité pour le

VIRTUALISATION DU RÉSEAU ÉTENDU (WAN)

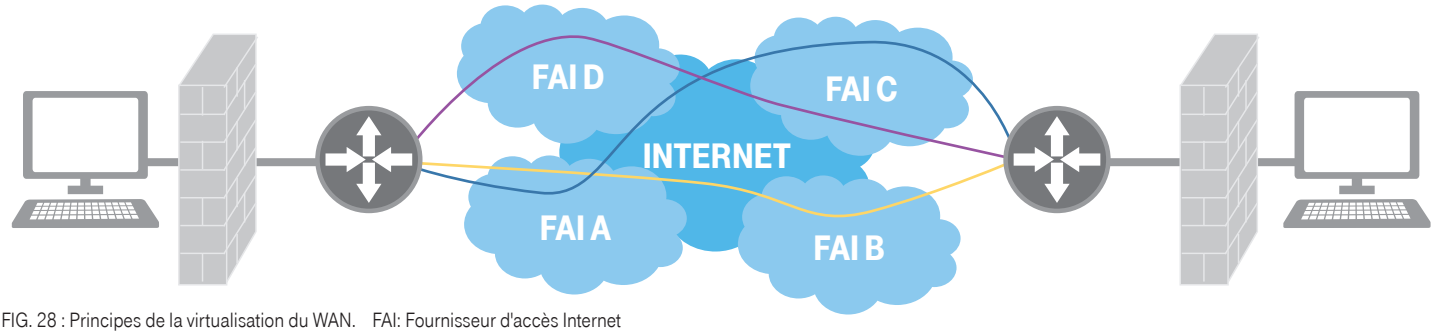


FIG. 28 : Principes de la virtualisation du WAN. FAI: Fournisseur d'accès Internet
Source : Deutsche Telekom

déploiement de services basés sur la NFV sera établie.

OPTIMISATION WAN

L'optimisation WAN est actuellement la méthode la mieux établie pour réduite les coûts liés à des réseaux d'entreprise. À l'origine, elle a été conçue pour rationaliser le trafic sur les réseaux MPLS, afin de maximiser le débit par rapport au coût. Aujourd'hui, l'agrégation des liaisons, le déchargement du trafic et le routage basé sur les performances prennent en compte Internet. L'objectif est passé de l'utilisation des connexions à un transfert de données efficace entre sites. Des méthodes telles que la déduplication et la compression des données, ainsi que l'optimisation de protocoles tels que le TCP, réduisent la quantité de données transférées par unité d'information, ce qui améliore le temps de réponse.

Sur les intranets uniquement sous MPLS, l'optimisation WAN est accomplie en déployant des terminaux adéquats sur le site du client (par exemple, des dispositifs de gestion des performances des applications).

EXIGENCES DE CONCEPTION DES RÉSEAUX

La présentation de Cisco en 2010, « Meilleures pratiques pour la conception de WAN d'entreprise » (Figure 29), répertorie les principaux critères pour la conception d'un réseau d'entreprise. Ces recommandations n'ont nullement perdu de leur pertinence et sont également applicables aux réseaux hybrides. La principale priorité des utilisateurs est et demeure une connexion haute disponibilité, suivie par la latence pour les applications hébergées dans des data centers ou des environnements cloud. Les fournisseurs de services réseau incluent ces critères dans leurs SLA, dans le cadre de leurs politiques de qualité de service. Le scandale des écoutes de la NSA, la fin de l'accord Safe-Harbor et l'utilisation croissance d'applications basées sur Internet ont fait de la sécurité des données une question de plus en plus sensible ces dernières années. L'intégrité des données (même lorsqu'elles sont transférées entre plusieurs plates-formes) doit être protégée par des méthodes vérifiables. Le chiffrement a donc un rôle important à jouer. Bien que cela ne figure pas dans les critères de Cisco, la conception d'un réseau à la fois rentable et sécurisé, est une priorité cruciale pour les DSI.

MEILLEURES PRATIQUES POUR LA CONCEPTION DE WAN D'ENTREPRISE

CONCEPTION HAUTE DISPONIBILITÉ
- CONNEXIONS AU WAN MULTIPLES/VARIÉES
- PFR POUR LE ROUTAGE INTELLIGENT DES APPLICATIONS

LATENCE ET OPTIMISATION DE LA BANDE PASSANTE
- MISE À NIVEAU DES POINTS D'AGRÉGATION À OC3/OC 12
- MISE À NIVEAU DES FILIALES À DS3 OU SUPÉRIEUR
- PLANIFICATION DE LA CAPACITÉ ET INGÉNIERIE DU TRAFIC
- MISE EN ŒUVRE DE LA MULTIDIFFUSION IP ET/OU DES SERVICES DE SEGMENTATION DE FLUX (PAR EX. WAAS)

DISTRIBUTION DES APPLICATIONS EN TEMPS RÉEL
- MISE EN ŒUVRE DE SOLIDES POLITIQUES DE QUALITÉ DE SERVICE POUR GÉRER LES NIVEAUX DE SERVICES DES APPLICATIONS
- ASSURER OU LIMITER LA CONSOMMATION DE LA BANDE PASSANTE SELON QU'ELLE SOIT SOUHAITABLE OU NON (COMME PISA)

ASSURANCE DE NIVEAU DE SERVICE
- SLA DU FOURNISSEUR DE SERVICES
- MISE EN ŒUVRE DES OUTILS DE GESTION DES SLA (PAR EX. NETFLOW, SLADES SERVICES SUR IP)

CONFIDENTIALITÉ
- SE CONFORMER AUX POLITIQUES DE SÉCURITÉ AVEC DES STRATÉGIES DE PROTECTION DES DONNÉES TELLES QUE IPSEC, DMVPN, GETVPN

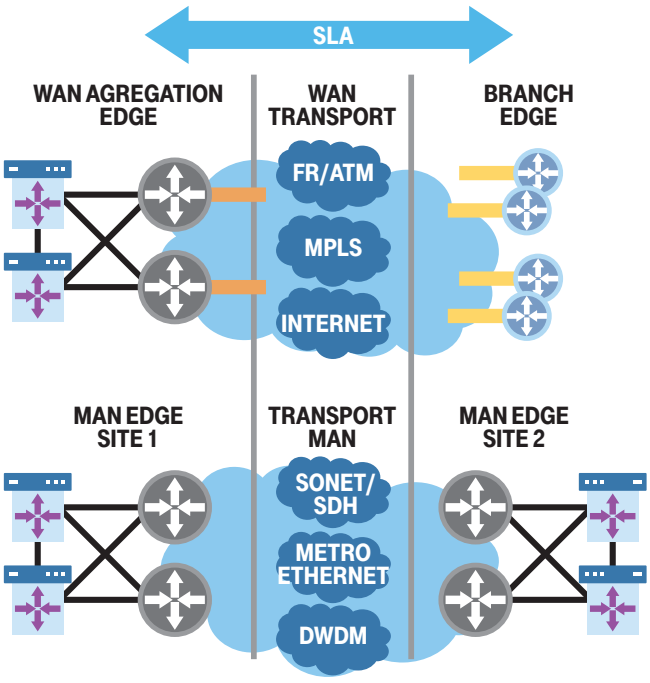


FIG. 29 : Meilleures pratiques pour la conception de WAN d'entreprise. Source : Cisco

Pour résumer, les exigences en matière de conception de réseau ont peu évolué ces dernières années. Sur le plan technique, le mélange d'applications de cloud public et privé, et les économies potentielles des réseaux hybrides soulèvent de nouvelles questions.

Connexions haute disponibilité

Avec la migration de plus en plus fréquente d'applications installées localement (comme Office 365) vers des plates-formes d'hébergement centrales (c'est-à-dire vers des data centers d'entreprise ou des clouds publics ou privés), la connectivité devient un paramètre crucial. Certaines applications peuvent être temporairement disponible hors connexion (grâce à des mécanismes de stockage asynchrone et à une mise en cache locale, par exemple). En revanche, les applications en temps réel (voix sur IP, WebEx, etc.) requièrent un échange de données ininterrompu avec le cloud.

Malheureusement, la relation entre disponibilité et coût d'une connexion n'est pas linéaire, les coûts s'élevant quasiment toujours de manière exponentielle. La raison est liée à la conception : la redondance (des chemins de sauvegarde secondaires ou même tertiaires, par exemple) est un vecteur de disponibilité. Comme l'accès au réseau est le principal facteur de coût, élever la disponibilité de 98,5 à 99,5 % peut aisément nécessiter le double du coût. Dans un tel contexte, les solutions plus abordables pour une redondance d'accès prennent une place importante dans la conception des réseaux hybrides. Les principales options sont :

- Utiliser des connexions de qualité inférieure (et à coût inférieur) comme chemin de sauvegarde
- Utiliser des réseaux mobiles payés selon l'utilisation
- Améliorer les performances
- Effectuer un déchargement du trafic

Cisco et un certain nombre de startups proposant des offres d'optimisation du trafic ont choisi de faire d'Internet la nouvelle plate-forme pour les réseaux d'entreprise. À la lumière de ses faibles coûts de bande passante, de la disponibilité globale, des capacités sensiblement supérieures, de la meilleure qualité, et de l'existence de technologies d'optimisation des performances éprouvées, les connexions Internet sont souvent considérées comme l'équivalent du protocole MPLS à biens des égards. Jusqu'à présent, le plaidoyer en sa faveur pour remplacer les plates-formes réseau plus onéreuses a eu une faible incidence sur l'utilisation du protocole MPLS comme base des réseaux d'entreprise, même si cela a eu, comme évoqué précédemment, des implications importantes pour la conception de l'accès au réseau. Internet prend donc de l'importance, et les clients attendent désormais des fournisseurs de services réseau qu'ils incorporent avec flexibilité des services Internet dans la conception de leurs réseaux d'entreprise pour leur offrir une haute disponibilité, des prix bas et une faible latence.

Temps de réponse du réseau

Dans les environnements cloud, la garantie du temps de réponse du réseau pour les applications sensibles aux délais telles que la téléphonie IP, devient une question cruciale à l'origine de nouveaux défis dans la conception des réseaux d'entreprise. Auparavant,, l'essentiel du trafic de données circulait des succursales vers un data center unique. Aujourd'hui, le trafic tend, au contraire, à être distribué entre plusieurs environnements de serveur. Par ailleurs, les applications de cloud public sont accessibles via des connexions Internet sécurisées ou des lignes Ethernet dédiées qui peuvent ne pas passer par le réseau principal. Pour cette raison, pour réduire la latence entre serveurs et succursales, le réseau doit proposer plusieurs chemins vers des clouds publics et privés, y compris en dehors du domaine (et donc hors du champ de contrôle direct de la plate-forme réseau principale). Ce résultat peut être obtenu de deux façons :

1. Un grand nombre de passerelles Internet, pour encourager l'acheminement du trafic vers la plate-forme réseau principale et offrir un certain niveau de contrôle du trafic,
2. Le routage basé sur les performances associé à des réseaux overlay, qui met en œuvre le contrôle du trafic à la périphérie du réseau et réduit par conséquent le rôle d'instance centrale de contrôle et de sécurité du réseau principal.

Ces deux modèles comportent des avantages et des inconvénients. On peut généralement s'attendre à ce que le routage basé sur les perfor-

mances soit utilisé sur les réseaux de nouvelle génération. De leur côté les offres basées sur le protocole MPLS sont davantage axées sur le déploiement d'un nombre de passerelles Internet suffisant pour réduire les délais sur les réseaux clients et continuer à utiliser la plate-forme MPLS comme instance de contrôle centrale.

Qualité de service

La popularité du MPLS sur les réseaux d'entreprise tient en partie à la qualité de service possible avec l'IP VPN. Celle-ci comprend deux composants : les classes de qualité et les gages de qualité. Le MPLS divise le trafic de données en catégories, chacune ayant un profil normalisé (catégorie de service) déterminant la manière dont est géré le trafic. Une catégorie de service est définie par une combinaison des attributs suivants : latence, pertes de paquets et instabilité (fluctuation de latence). Des SLA peuvent garantir des seuils pour tout ou partie de ces attributs (gages de qualité) en s'appuyant sur des politiques de régulation des files d'attente et du trafic, mises en oeuvre dans les noeuds. Les fournisseurs peuvent ainsi offrir des garanties sur les performances des applications critiques, et assurer leur réactivité et leur facilité d'utilisation.

Le modèle de qualité de service a une application limitée sur les réseaux hybrides. En premier lieu, seul le fournisseur a une influence indirecte sur la qualité de transmission dans les parties d'un réseau hybride basées sur l'Internet public. Ensuite, les mécanismes d'acheminement dynamique du trafic tels que le routage basé sur les performances envoient des données dans un ensemble de réseaux ayant des caractéristiques de qualité hétérogènes. Les fournisseurs utilisant des méthodes de gestion conventionnelles sont alors incapables de prédire le comportement du trafic dans tout le réseau d'entreprise. Pour cette raison, les définitions de qualité de service utilisées sur les réseaux MPLS ne peuvent s'appliquer qu'aux parties d'un réseau basées sur l'infrastructure MPLS et prenant en charge des capacités de gestion et de hiérarchisation du trafic. Dans le cas de réseaux overlay, de telles méthodes ne peuvent avoir qu'un usage limité (voire nul), ce qui rend difficile, ou impossible, de garantir des paramètres de qualité du trafic aux clients. Le problème de la gestion du trafic est la raison pour laquelle nombre d'entreprises continuent à utiliser des mécanismes MPLS pour les applications sensibles à la latence comme la voix et la vidéo. Il n'existe actuellement pas d'autre moyen de satisfaire les attentes des utilisateurs.

La définition et la structure de la qualité de service sur les réseaux d'entreprise sont susceptibles d'évoluer à l'avenir pour permettre l'application de gages de qualité de service aux réseaux hybrides. Dans le modèle MPLS, la hiérarchisation du trafic des applications est basée sur les adresses IP et les numéros de port de couche 4. Elle est accomplie grâce à des fonctions de mise en attente, de modélisation et d'acheminement du trafic. En revanche, sur les réseaux hybrides, ce sont les applications qui sont analysées et classées selon la nature de leur trafic de données. Contrairement au MPLS, ce processus peut être configuré de façon dynamique depuis une instance de gestion centrale. Sur les réseaux hybrides, le routage basé sur les performances et l'optimisation du trafic remplacent la mise en file d'attente, la modélisation et l'acheminement pour garantir des performances réseau appropriées pour toutes les applications. La priorité n'est plus la gestion des goulots d'étranglement de la bande passante et la hiérarchisation du trafic de données, mais la latence du réseau et la recherche des chemins de transfert les plus directs.

L'optimisation du trafic fait déjà partie intégrante de nombreux réseaux d'entreprise, et un certain nombre de solutions logicielles permettent de gérer et de configurer le comportement des applications sur des réseaux hybrides. Citons notamment iWAN de Cisco et le service de sélection de chemin de Riverbed. Jusqu'à présent, les fournisseurs de services réseau sont peu enclins à incorporer des logiciels d'optimisation du trafic dans leurs plates-formes. Cette réticence ralentit la transition du MPLS au modèle hybride.

Dans les prochaines années, nous devrions assister à l'émergence d'un mélange de produits basées sur le MPLS pour les applications telles que la VoIP, la vidéo et les bureaux distants, et de produits hybrides pour tous les autres types de données et applications. Les organisations continueront à exploiter les avantages du premier en matière de qualité de service pour leurs applications critiques, tout en transférant une grande partie de leur trafic de données sur d'autres plates-formes (principalement Internet). Mais il n'est pas encore possible de savoir si ce scénario d'utilisation parallèle sera utilisé sur le long terme ou s'il s'agira juste d'une phase de transition vers des réseaux basés sur la NFV et le SDN. Dans ce dernier cas, les fournisseurs de MPLS devront élaborer une stratégie pour transformer leurs plates-formes réseau (ainsi que leurs systèmes d'exploitation et métiers) afin de prendre en charge les technologies de demain.

SLA

Les SLA des réseaux MPLS sont extrêmement normalisés et très similaires pour tous les acteurs du domaine. Cela tient avant tout à la structure des portefeuilles basés sur le MPLS et, ensuite, aux exigences définies par les clients (spécifiées dans le cadre d'appels d'offres).

Deux types de niveaux de service sont communs aux réseaux MPLS :
1. Gestion de la livraison et des changements
2. Qualité de la transmission

Fourniture de services réseaux
Le respect de la date de livraison confirmée (à savoir, la date à laquelle le réseau est prêt à l'emploi) est habituellement la seule exigence définie dans la catégorie "gestion de la livraison et des changements". Les SLA définissent une date concrète à laquelle le fournisseur garantit l'ouverture de la connexion au client. Par voie de conséquence, cela signifie qu'ils ne s'appliquent pas aux périodes du processus de livraison qui ne sont pas sous le contrôle du fournisseur.

Tout cela est généralement lié à la mise en œuvre du dernier kilomètre : le fournisseur du dernier kilomètre peut rarement s'engager sur une date fixe, sauf peut-être dans le cas de connexions de téléphones cellulaires où des cartes SIM ou des comptes d'accès au réseau peuvent être fournis quasiment instantanément. Par conséquent, dans la plupart des cas, il n'est possible de fournir une date d'achèvement fixe d'un réseau MPLS qu'une fois le dernier kilomètre mis en œuvre, et la date de livraison du routeur interne du client connue. De ce fait, du point de vue du client, la définition d'un paramètre prêt à l'emploi n'offre qu'un avantage limité pour les réseaux MPLS basés sur des connexions terrestres et sur Internet.

Notons cependant que les réseaux de nouvelle génération (basés sur la technologie du SDN) modifieront largement la perception de retard de transmission du réseau. Aryaka, et d'autres, affirment d'ailleurs que les leurs peuvent être fournis instantanément, en quelques clics, sur un portail Web, ce qui est possible avec une connexion Internet active déjà en déploiement et lorsque le matériel générique du fournisseur de services réseau (basés sur x86) a déjà été connecté sur le site du client.
Avec cette configuration, le terminal peut en effet être fourni avec toutes les options de configuration réseau proposées par le fournisseur sur son portail. Toutefois, si le client exige du fournisseur qu'il installe également l'accès au réseau à proprement parler, le problème du calendrier de livraison demeure inchangé par rapport à celui des plates-formes réseau basées sur MPLS.

Qualité de transmission des réseaux hybrides
La qualité de service garantie, différenciée selon le type d'application, est l'un des arguments en faveur du MPLS. Le fournisseur peut, par exemple, garantir la qualité de la communication VoIP quand la configuration adéquate est en place, ce qui n'est actuellement pas possible avec d'autres types d'IP VPN, en particulier dans le cas de connexions basées sur Internet. La garantie de qualité de service est une combinaison des indicateurs suivants :

- Latence des données sur le réseau
- Instabilité (Jitter)
- Taux de perte de paquets

Les fournisseurs réseau mesurent et documentent ces trois indicateurs, et des sanctions contractuelles définies dans les SLA s'appliquent en cas de non-conformité.
Comme les réseaux hybrides mélangent différentes plates-formes, les niveaux de service garantis pour les données MPLS ne peuvent pas être appliqués au trafic Internet. Internet est donc décrit comme une plate-forme répondant davantage à une « obligation de moyens ». Cela signifie que tous les paquets entrants doivent être transmis dans les plus brefs délais, selon les ressources disponibles. Si les capacités du réseau sont épuisées, des goulots d'étranglement se produisent, et il n'existe plus aucune garantie de transmission complète et sans erreur. De nombreux fournisseurs de services d'optimisation des performances affirment qu'ils peuvent modifier les flux de trafic de manière à ce que la qualité du trafic de données Internet corresponde ou même surpasse celle des réseaux MPLS.

Cette affirmation est fondée dans la plupart des cas. Toutefois, les opérateurs évitent de prendre des engagements contraignants ou de donner des garanties quant au comportement des applications sur les réseaux hybrides, car ils n'exercent pas un contrôle total sur la qualité de transmission. On peut comparer cela à l'incidence du dernier kilomètre sur les dates de livraison d'une connexion réseau MPLS.

La qualité de service du trafic de données est le principal critère des réseaux MPLS. Pour les réseaux hybrides, l'accent est mis sur les performances des applications. Les décisions de routage sont en effet automatisées entre plusieurs plates-formes. Sur un réseau MPLS, la configuration des flux de données est statique, tandis que dans les environnements hybrides, la configuration est dynamique et orientée applications. Les fournisseurs peuvent continuer à inclure des SLA relatifs au trafic pour la partie MPLS des réseaux d'entreprise. Toutefois, ceux-ci ne fournissent aucune indication fiable sur les performances des applications. Dans un scénario hybride, si une application entraîne une perte de performance temporaire, il est souvent impossible d'en déterminer la cause principale. Elle peut être imputable au réseau MPLS ou au routage temporaire des données via une connexion Internet de qualité inférieure. Même si le fournisseur vérifie les informations de routage et peut prouver le respect de la qualité de service définie pour la partie MPLS du réseau d'entreprise, le client n'en tire aucun avantage réel. Ils continueront à n'avoir qu'un contrôle limité sur le comportement des applications.

L'accès aux applications via Internet dans des environnements de cloud public est à l'origine d'un problème supplémentaire au niveau des SLA traditionnels des réseaux MPLS. Le fournisseur n'ayant pas le contrôle total sur le comportement des applications sur Internet, l'inclusion d'un indicateur correspondant dans les SLA serait donc un pari risqué. Des mécanismes d'optimisation des performances peuvent être mis en œuvre, mais il est impossible de fournir la moindre garantie sur les performances des applications dans des data centers de cloud public. Cela diminue encore intrinsèquement la valeur des SLA pour le client.

Implications pour l'avenir des SLA

Actuellement, les SLA des réseaux MPLS sont l'une des raisons pour lesquelles les entreprises rechignent à adopter des VPN basés sur Internet pour remplacer la totalité de leurs infrastructures réseau. Toutefois, les économies importantes, la meilleure qualité de transmission des données sur Internet et la disponibilité généralisée des technologies d'optimisation des performances encourageront la migration vers des réseaux hybrides dans un avenir proche. Les utilisateurs de réseaux hybrides cherchent donc une nouvelle approche normalisée vis-à-vis de leurs SLA.. Conjointement aux applications hébergées dans le cloud, on verra probablement émerger des garanties complètes spécifiques au domaine des TIC, comprenant une description du comportement des applications au niveau de l'utilisateur, et incluant les performances réseau. Ces nouveaux SLA incluront les paramètres suivants :

- **Vitesse d'approvisionnement**

Le passage des réseaux MPLS conventionnels aux réseaux hybrides avec une fonctionnalité de gestion basée sur la NFV ou le SDN devrait avoir une incidence sur la vitesse d'approvisionnement. À l'avenir, les clients exigeront des fournisseurs de réseau de pouvoir activer et désactiver les services de transport en quelques minutes – au moins sur les connexions Internet existantes.

- **Disponibilité de l'application au niveau de l'utilisateur dans le temps**

Pour garantir la disponibilité de l'application, le fournisseur de services réseaux doit non seulement gérer la connexion au data center du fournisseur de services cloud, mais aussi obtenir des garanties (accords de niveau d'exploitation) de ce dernier sur la disponibilité de l'application dans le data center. La gestion technique de ces deux aspects interdépendants fait encore l'objet de débats. Toutefois, les fournisseurs de services cloud sont très intéressés par la possibilité de connecter directement leurs data centers aux plates-formes des fournisseurs de réseaux d'entreprise. Ce qui indique clairement que des SLA de ce type sont susceptibles d'émerger dans un futur proche.

La latence des applications sur Internet deviendra de plus en plus critique, augmentant ainsi l'importance des paramètres réseau associés. Les fournisseurs de services réseaux et les clients doivent donc convenir de la façon dont ces paramètres doivent être régis dans les SLA. Ceux-ci devront, comme toujours, être mesurables et documentés. Toutefois, il faudra trouver le juste équilibre entre le contrôle limité du fournisseur sur certains paramètres, et les attentes des clients. Il est également probable que ces SLA évoluent progressivement pour tenir compte des capacités de supervision et de contrôle des logiciels de gestion des performances des applications.

Protection des données

La protection des données est un autre défi majeur des réseaux hybrides complexes. L'adoption de clouds publics et privés crée d'ores et déjà de nouveaux impératifs de protection des données, car les entreprises ont très peu de contrôle sur les solutions cloud de sécurité. Alors que les fournisseurs de cloud privé conviennent de paramètres tels que l'emplacement géographique du stockage de données et la protection du système d'information avec chaque client, chaque opérateur de cloud public met en œuvre ses propres mécanismes de sécurité. Ceux-ci ne sont souvent ni comparables ni suffisamment transparents.

La protection des données est également un problème complexe pour les réseaux d'entreprise. Les données circulent non seulement d'un site du réseau à un autre, mais également entre l'environnement d'entreprise et le cloud public. Les communications avec le cloud public peuvent être statiques ou dynamiques, et protégées de diverses manières. L'échange de données via Dropbox, par exemple, est initié par les utilisateurs de manière dynamique et protégé par des tunnels SSL. En revanche, les applications qui se trouvent dans un PaaS Amazon, sont accessibles via des tunnels IPSec statiques depuis l'interface vers Internet. Le nombre croissant d'applications distribuées via des clouds publics et des passerelles Internet éparses complique la mise en oeuvre, la gestion, le maintien et l'actualisation de normes de sécurité cohérentes sur un réseau.

Tout cela nuit à l'adoption de réseaux hybrides. Toutefois, les services de sécurité existants sont amenés à s'améliorer et à entraîner une plus grande confiance dans les réseaux hybrides et les scénarios de cloud. Enfin, les coûts inférieurs et le vaste choix d'applications professionnelles sur les clouds publics persuaderont également de plus en plus d'entreprises à migrer. En phases de transition, les fournisseurs de services réseaux peuvent enrichir leurs portefeuilles en y intégrant des systèmes de sécurité prenant en charge les réseaux hybrides. Cela les aidera à protéger leur position sur le marché sur le long terme. Clairement, les mécanismes de sécurité des réseaux hybrides devront être une fonctionnalité standard des portefeuilles de demain.

Modèles d'exploitation

Les réseaux hybrides exigent de nouveaux modes de fonctionnement et d'exploitation. Cela s'applique aussi bien aux systèmes de support opérationnel (OSS) qu'à leurs cousins, les systèmes de support fonctionnel (BSS). Les OSS sont des systèmes de gestion de réseaux qui prennent en charge des processus automatisés, comme la gestion des erreurs, des configurations ou de la comptabilité. Les BSS prennent en charge les processus commerciaux, tels que la gestion des relations entre client et fournisseur ou les tâches administratives internes. Des changements s'imposent pour plusieurs raisons :

- Les attentes au niveau des portails de gestion des réseaux en libre-service évoluent. À l'avenir, les portails ressembleront aux environnements de configuration déjà courants pour les offres PaaS et IaaS de cloud public. Les principales améliorations seront un approvisionnement plus rapide, et davantage de responsabilisation du client pour la configuration.
- Les réseaux overlay suscitent de plus en plus d'intérêt en raison de leur capacité d'intégration fluide et personnalisée de plusieurs plates-formes réseau.
- Les méthodes de surveillance des réseaux et de gestion du trafic évoluent à partir de mécanismes typiques (basés sur IP et sur des ports) des plates-formes MPLS vers des systèmes ressemblant à des logiciels de gestion des performances des applications.
- La conception du réseau devra inclure l'intégration sans accroc de systèmes de sécurité des données propres au client, ce qui n'existait jusqu'ici qu'en option.

Certains réseaux hybrides de première génération peuvent être associés à des OSS/BSS existants. Mais la mise en œuvre d'architectures NFV ou SDN requiert de faire table rase des SLA existants pour reprendre à zéro. Les technologies NFV et SDN prennent en charge la configuration de réseau hautement dynamique. Un régulateur logiciel central approvisionne les terminaux (une tâche qui peut, dans certains cas, être initiée par le client ou l'utilisateur). Le matériel correspondant sur site, lui, est générique. Des études menées par TM Forum, une association mondiale du secteur de l'économie numérique, montrent que l'incidence de ces changements techniques sera significative et nécessitera une transformation des OSS et BSS, ainsi que des processus associés.

Intégration d'Internet dans des plates-formes MPLS

Les fournisseurs de services réseaux peuvent améliorer leurs offres MPLS existantes pour y inclure des éléments hybrides en exploitant Internet comme un mode d'accès ou un service à valeur ajoutée. Les entreprises incluent d'ailleurs déjà l'intégration d'Internet dans leurs appels d'offre pour la conception de réseau. Les exigences classiques incluent :

- Le déchargement du trafic
- Le routage basé sur les performances
- Le contrôle de séparation des flux (split tunneling)
- Les connexions aux plates-formes de cloud public
- L'accès à Internet sécurisé depuis les sites des clients

Les principaux objectifs sont de réduire les coûts (en fournissant plus de bande passante pour moins d'argent) et la latence entre le site du client et les applications dans le cloud public. Les fournisseurs de services réseaux peuvent, une fois encore, satisfaire à ces exigences de deux manières :

1. En créant un grand nombre de passerelles vers Internet ou
2. En autorisant l'accès à Internet sur les terminaux

Les critères commerciaux détermineront quelle méthode ou combinaison de méthodes seront incluses dans les offres des fournisseurs.

Intégration du cloud dans des plates-formes MPLS

Les plates-formes MPLS peuvent également être améliorées au travers de connexions directes à des environnements de cloud public. Dans de tels scénarios, la plate-forme cloud est accessible via une passerelle cloud sur le réseau d'entreprise. Cette configuration n'exige pas forcément la mise en œuvre d'éléments de connexion propres au réseau ou, si la passerelle mène à un environnement de cloud privé, l'installation de systèmes de sécurité. Dans une large mesure, la conception de la passerelle entre les plates-formes MPLS et cloud peut être basée sur le type d'interface de réseau à réseau (NNI) utilisé pour les interconnexions multilocataires entre les réseaux MPLS. À condition d'avoir suffisamment de bande passante disponible pour la passerelle, des mécanismes QoS et CoS pourraient être inutiles. Mais les fournisseurs de réseaux MPLS doivent résoudre deux autres problèmes :

1. La répartition géographique des passerelles
2. Le choix des fournisseurs de services cloud

Les environnements de cloud public sont généralement répartis sur plusieurs régions. Les utilisateurs d'applications s'enregistrent dans une région spécifique et accèdent à leurs données depuis cette région. Par exemple, un individu à Sydney utilisera sans doute les serveurs prévus pour l'Australie et la Nouvelle-Zélande, alors qu'un autre se trouvant à Londres aura accès aux serveurs situés en Europe de l'ouest. Cette répartition géographique est importante, à la fois pour réduire la latence entre les serveurs et les sites des clients, et pour respecter les législations nationales. Dans certains cas, les fournisseurs de services réseaux ayant des clients à l'international doivent mettre en œuvre des passerelles vers le même fournisseur de services cloud dans plusieurs régions. Dans la pratique, la répartition des passerelles dépend des exigences du client et de la plate-forme cloud spécifique.

MARCHÉ DES INFRASTRUCTURES CLOUD – PARTS DE MARCHÉ MONDIALES 2015

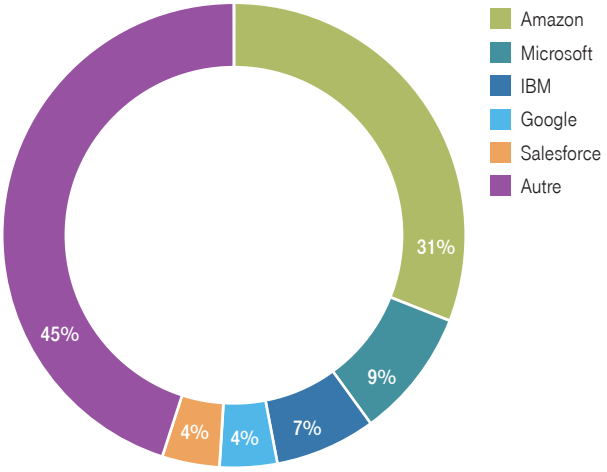


FIG. 30 : Les quatre principales entreprises totalisent plus de la moitié du marché des infrastructures cloud dans le monde (y compris le IaaS, le PaaS, le cloud privé et le cloud hybride). Source : Synergy Research Group

Il n'est pas facile pour les opérateurs d'identifier quels fournisseurs de services cloud devraient disposer d'une connexion directe vers une plate-forme MPLS donnée, ou en d'autres termes, à quels fournisseurs de services cloud se connectent vraiment les clients. Le marché de l'IaaS, du PaaS et du SaaS est fragmenté, avec un flux permanent de nouveaux arrivants (Figure 30). Une solution consiste à exploiter les points d'appairage pour les environnements cloud hébergés par des opérateurs comme Equinix. Une passerelle entre la plate-forme MPLS et le point d'appairage donne accès à tous les fournisseurs de clouds publics enregistrés simultanément. Cela réduit les coûts de passerelle pour le fournisseur de services MPLS. Toutefois, l'utilisation de ces points d'échange génère des coûts permanents. Plus ces coûts sont élevés, moins l'appairage devient attractif. Du point de vue de la rentabilité, l'approche typique consiste à combiner des passerelles directes vers les principales plates-formes cloud (du point de vue de l'opérateur réseau) avec des connexions vers des points d'échange. Comme évoqué précédemment, il a été établi que la plupart des fournisseurs de services réseaux internationaux se connectent au moins à Amazon (IaaS, PaaS), Microsoft (PaaS et SaaS), Google et souvent aussi à Salesforce (SaaS).

PERSPECTIVE

La technologie MPLS restera un élément essentiel des réseaux d'entreprise pour les trois prochaines années. Le marché devrait se stabiliser en raison de la demande croissante en services réseaux de façon générale, et devrait même connaître une légère reprise avec l'augmentation de la part du trafic transférée vers des infrastructures WAN (notamment pour la voix sur IP et les vidéoconférences).

Toutefois, le rôle des plates-formes MPLS devrait évoluer à moyen terme. Le besoin en bande passante et d'accès au cloud public va continuer à croître, ce qui augmentera en retour l'attrait du déchargement du trafic ou encore du routage haute performance. À l'avenir, les entreprises chercheront à créer des réseaux d'entreprise haute performance mais rentables, et adaptés à leurs besoins. Dans un tel contexte, Internet va faire partie intégrante de l'environnement réseau, aux côtés et en complément de la technologie MPLS. Les fournisseurs doivent donc désormais étendre leurs plates-formes et leurs portefeuilles MPLS pour y inclure des services Internet, de routage haute performance, et des solutions de sécurité. Cette tendance est assez marquée ces dernières années et va continuer à prendre de l'ampleur. Autre tendance : la demande croissante pour un accès rapide et sécurisé au cloud. En réponse, de nombreux fournisseurs de services réseaux à l'international travaillent à l'incorporation d'interfaces vers des leaders du cloud tels que Microsoft et Amazon. L'accès direct au cloud depuis un réseau MPLS privé représente en effet une valeur ajoutée pour les entreprises, car il offre davantage de sécurité, de fiabilité et de qualité qu'Internet. Il permet également une intégration sans accroc du cloud dans l'environnement professionnel. Outre le MPLS et Internet, Ethernet sera une autre composante essentielle de l'infrastructure de base des solutions réseau intégrées (Figure 31).
À long terme, le software-defined networks (SDN) et la NFV occuperont une place dominante dans les réseaux privés. Ces technologies sont déjà suffisamment avancées pour servir de bases à de nouveaux réseaux. Toutefois, en raison de différences radicales entre les réseaux MPLS et SDN, il faudra encore plusieurs années aux opérateurs pour migrer leurs plates-formes actuelles vers la nouvelle architecture. Il s'agira forcément d'une entreprise à long terme, compte tenu de facteurs tels que la protection des investissements pour les plates-formes existantes, la nécessité d'une nouvelle stratégie de portefeuille, les coûts de développement élevés des nouvelles plates-formes, et la gestion des risques. Dans le même temps, de nombreuses startups agiles établissent des réseaux multinationaux basés sur le SDN. Plus flexibles que les opérateurs en place, elles n'ont pas à tenir compte des structures organisationnelles ou des environnements informatiques existants, ce qui leur confère un avantage lors de la mise en œuvre de la technologie SDN. Cependant, il leur manque l'infrastructure réseau nécessaire pour concurrencer les principaux acteurs internationaux. Elles sont ainsi désavantagées quand elles tentent de gagner la confiance des clients des opérateurs en place. À moyen terme, on peut s'attendre à ce qu'elles se concentrent sur un segment de niche qui empiètera à peine sur le marché occupé par les acteurs internationaux établis. Sur le long terme, toutefois, les différences entre les portefeuilles des deux groupes devrait s'estomper. Pour les opérateurs en place, cela pourrait signifier une perte de parts de marché au profit de nouveaux entrants.

PRÉVISIONS POUR LE MARCHÉ DES VPN

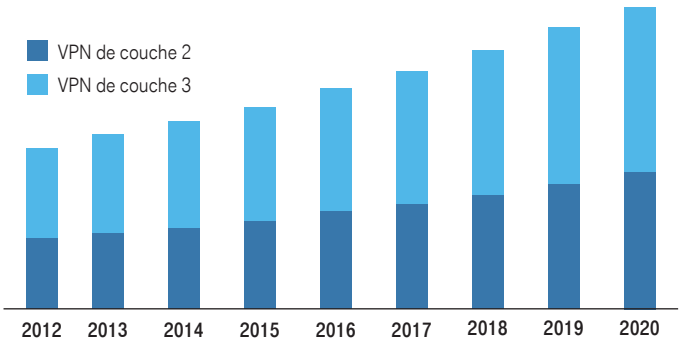


FIG 31 : Évolution du marché des VPN (couche 2, couche 3).
Source : GrandView Research

À terme, les marchés de l'informatique et des télécommunications fusionneront totalement. Avec la virtualisation croissante des technologies de télécommunications (c'est-à-dire, le remplacement du matériel par du logiciel), les fournisseurs de services réseaux seront contraints d'acquérir de nouvelles compétences et de repenser leurs processus et leurs structures organisationnelles. Ainsi, les fournisseurs ont le choix entre deux stratégies :

1. Devenir les leaders de la fourniture de services réseaux à l'international en termes de coût et de qualité (stratégie de fournisseur d'infrastructure)
2. Devenir des fournisseurs de services cloud intégrés, en incluant les services réseaux correspondants (stratégie d'intégrateur)

CHIFFRES ET SOURCES

FIG. 1 UTILISATION DU CLOUD HYBRIDE PAR LES ENTREPRISES
http://www.informationweek.com/cloud/infrastructure-as-a-service/hybrid-cloud-all-about-the-network/a/d-id/1298152

FIG. 2 STRATÉGIES DE CLOUD D'ENTREPRISE, RAPPORT SUR L'ÉTAT DU CLOUD
http://assets.rightscale.com/uploads/pdfs/RightScale-2014-State-of-the-Cloud-Report.pdf

FIG. 3 OBSTACLES À LA MISE EN ŒUVRE DU CLOUD COMPUTING EN ENTREPRISE
http://www.computing.co.uk/ctg/analysis/2230812/cloud-computing-the-lessons-learned

FIG. 4 TRAFIC IP DANS DES DATA CENTERS DE CLOUD
https://timedotcom.files.wordpress.com/2015/05/cloud_index_white_paper.pdf

FIG. 5 CONNEXIONS AU SEIN DES RÉSEAUX HYBRIDES D'ENTREPRISE

FIG. 6 REPARTITION DU TRAFIC IP DANS UN DATA CENTER CLOUD
https://timedotcom.files.wordpress.com/2015/05/cloud_index_white_paper.pdf

FIG. 7 LES RESSOURCES DES DATA CENTERS VIRTUELS DESTINÉES À DIFFÉRENTES UNITÉS ADMINISTRATIVES VIENNENT DE POOLS DE CLOUDS
http://www.equinix.de/locations/americas-colocation/americas-data-centers/

FIG. 8 CONCEPTION EN ÉTOILE DES RÉSEAUX D'ENTREPRISE
T-Systems

FIG. 9 PROJECTION DU NOMBRE D'ABONNEMENTS SOUSCRITS PAR DES UTILISATEURS FINAUX À UN SERVICE CLOUD DANS LE MONDE (EN MILLIONS)
https://technologie.ihs.com/410084/subscriptions-to-cloud-storage-services-to-reach-half-billion-level-this-year

FIG. 10 TRAFIC DE DONNÉES CLOUD PAR APPLICATION
https://www.skyhighnetworks.com/cloud-report/

FIG. 11 NOMBRE D'APPLICATIONS SUR LES RÉSEAUX D'ENTREPRISE
https://www.skyhighnetworks.com/cloud-report/

FIG. 12 TAUX DE BLOCAGE D'APPLICATIONS RÉEL ET VISÉ SUR LES RÉSEAUX D'ENTREPRISE
https://www.skyhighnetworks.com/cloud-report/

FIG. 13 LA MENACE PERÇUE ET INCIDENTS DE SÉCURITÉ RÉELS IMPUTABLES À DES ACTEURS INTERNES D'UNE ENTREPRISE
https://www.skyhighnetworks.com/cloud-report/

GLOSSAIRE ET ABRÉVIATIONS

API	Application programming interface	Interface de programmes d'applications
ATM	Asynchronous transfer mode	Mode de transfert asynchrone
AWS	Amazon Web Services	Amazon Web Services
BSS	Business support systems	Systèmes de support fonctionnel
BW	Bandwidth	Bande passante
CAGR	Compound annual growth rate	Taux de croissance annuel composé
CAPEX	Capital expenditure	Dépenses d'investissement
CDN	Content delivery network	Réseau de diffusion de contenu
CE	Customer edge router	Routeur périphérique client
CIO	Chief Information Officer	Directeur des systèmes d'information (DSI)
CoS	Class of service	Catégorie de service
CPU	Central processing unit	Unité de traitement centrale (UC)
CSP	here: Communication service provider	ici : Fournisseur de services de communication
DDoS	Distributed denial of service	Déni de service distribué
DSL	Digital subscriber line	Ligne d'abonné numérique
GCE	Google Compute Engine	Google Compute Engine
GRE	Generic routing encapsulation	Encapsulage générique de routage
HTTP	Hypertext transfer protocol	Protocole de transfert hypertexte
IAAS	Infrastructure as a service	Infrastructure sous forme de service
IP Sec	Internet protocol security	Protocole de sécurité IP

IP VPN	Internet protocol virtual private network	Réseau privé virtuel IP
ISP	Internet service provider	Fournisseur de services Internet
ICT	Information and communications technologies	TIC (technologies de l'information et de la communication)
LAN	Local area network	Réseau local
ELT	Long-Term Evolution	Technologie d'évolution à long terme
MPLS	Multi-protocol label switching	Commutation multiprotocole par étiquette
NFV	Network function virtualization	Virtualisation des fonctions réseau
Ngena	Next Generation Network Alliance	Next Generation Network Alliance
NNI	Network-network interface	Interface de réseau à réseau
OPEX	Operational expenditure	Dépenses d'exploitation
OSS	Operations support systems	Systèmes de support opérationnel
PAAS	Platform as a service	Plate-forme sous forme de service
PoP	Point of presence	Point de présence
POP3	Post office protocol	Protocole POP
RAM	Random-access memory	Mémoire vive
R&D	Research & development	Recherche et développement
RFP	Request for proposal	Appel d'offres
ROI	Return on investment	Retour sur investissement
ROM	Read-only memory	Mémoire morte
SAAS	Software as a service	Logiciel comme service

SDN	Software-defined networks	Software-defined networks
SLA	Service level agreement	Accords de niveau de service
SSL	Secure socket layer	Secure socket layer
VoIP	Voice over Internet protocol	Voix sur IP
VPN	Virtual private network	Réseau privé virtuel
WAN	Wide area network	Réseau étendu

CONTACT

Marketing
T-Systems International GmbH
Uli Kunesch
Intelligence marketing
Fasanenweg 5
70771 Leinfelden-Echterdingen
Allemagne
Uli.Kunesch@t-systems.com

Responsable du contenu
T-Systems North America, Inc.
Christian Thun
International Solution Sales TC
1 Rockefeller Plaza, 16th Fl
New York, NY 10020
USA
Christian.Thun@t-systems.com

PUBLIÉ PAR

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main
Allemagne
www.t-systems.com

Dernière mise à jour avril 2016

T · · Systems ·