
Le guide de
la connectivité
au cloud public
en datacenter
TELEHOUSE

Le guide de la connectivité au cloud public en datacenter

Édito

Aujourd'hui, les organisations ont parfaitement compris les atouts du cloud et la grande majorité l'utilise. Le cloud s'impose en particulier par le biais des stratégies dites « cloud first » consistant à passer un maximum de workloads – voire tous – dans le cloud.

Qui dit cloud first, dit déplacement de l'usage du cloud de la périphérie vers le cœur de l'environnement IT, c'est pourquoi la connexion au cloud public devient un enjeu toujours plus stratégique.

Or, pour de nombreuses entreprises, plusieurs interrogations demeurent sur les meilleures modalités de connexion garantissant aux utilisateurs finaux un accès sans faille aux services. Quelle route privilégier, à quel coût, pour quelle performance et avec quel niveau de sécurité : répondre à toutes ces questions implique de bien cerner les différents modèles de connexion au cloud.

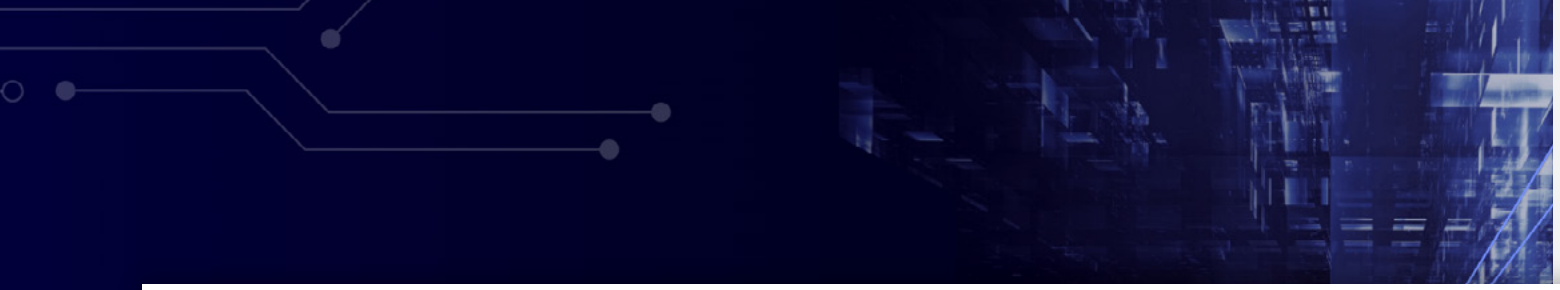
Ce livre blanc présente les trois modes de connexion au cloud public disponibles dans un datacenter de connectivité, leurs atouts et les points d'attention qu'ils soulèvent.

Notre objectif : vous guider vers le meilleur choix d'accès au cloud public selon les contraintes de réseau et de trafic de votre entreprise, ses compétences techniques et ses budgets.

Nous vous en souhaitons bonne lecture.

Sami Slim
Deputy Sales Director,
Telehouse France

Sommaire



L'essentiel

La question de la connexion au cloud public se pose d'autant plus que les entreprises orientent leurs applications vers une architecture cloud suivant des stratégies cloud-first et multicloud.

Dans ce contexte, une présence dans un datacenter hautement connecté permet d'avoir à portée de main – et de câble – plusieurs options de connexion au cloud public. Selon les caractéristiques de son trafic, une entreprise peut ainsi adapter sa connexion à ses contraintes, mais aussi composer avec plusieurs modes d'accès au cloud :

Le cross-connect tire parti de la grande densité de membres du datacenter de connectivité qui permet d'établir un câblage direct entre le routeur d'une entreprise et celui d'un opérateur cloud, d'où une connexion sécurisée, sans aucun intermédiaire ;

Les liens managés sous forme de solution NaaS (réseau à la demande) permettent une connectivité au cloud sécurisée et à la demande vers un ou plusieurs fournisseurs, souplesse et simplicité du modèle en prime ;

Le peering public, via l'Internet public, permet un échange de trafic vers plusieurs fournisseurs en interconnectant directement les réseaux de l'entreprise et du fournisseur cloud – de quoi assurer rapidement une connexion très qualitative, sans fort engagement contractuel.

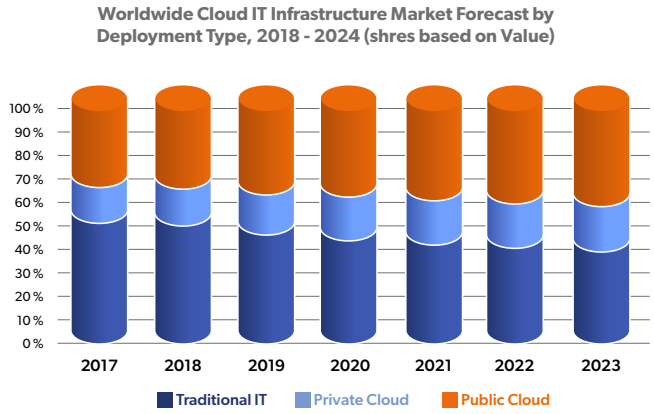
1. Le cloud public, pilier des stratégies « cloud first »

Les entreprises orientent de plus en plus leurs applications vers une architecture native cloud afin de tirer parti plus rapidement des nouvelles technologies de l'information et de l'agilité associée. Ce choix se reflète dans leurs dépenses : IDC note qu'en 2019, les dépenses en infrastructure informatique cloud ont dépassé les dépenses en infrastructure informatique non cloud. Ses analystes prévoient que l'infrastructure informatique cloud reste au-dessus de 50 % du marché de l'infrastructure informatique aux niveaux trimestriel et annuel, atteignant une part de 60,5 % par an en 2024[1].

La tendance cloud first est confirmée par Gartner également qui évalue que plus de 75 % des entreprises utilisatrices du cloud suivent une stratégie cloud first. Dans ce contexte, le cloud public reste en tête des investissements : selon IDC, au 4e trimestre 2019, la croissance des dépenses mondiales dans l'infrastructure informatique cloud a été tirée par le segment du cloud public qui atteint 13,3 milliards de dollars (+14,5 % en un an, comparé à +8,2 % des dépenses dans le cloud privé atteignant 6,1 milliards de dollars). Sur toute l'année 2019, les dépenses mondiales sur le segment du cloud public ont atteint 45,2 milliards de dollars en 2019, contre 21,6 milliards pour le cloud privé. Si la hausse annuelle est, au final, plus forte pour le cloud privé (+6,6 % contre + 0,1 % pour le cloud public), le cloud public reste en position de force pour servir les stratégies cloud first des entreprises. Aussi, les enjeux de connectivité au cloud public résident au cœur de ces stratégies.

75 % des entreprises utilisatrices du cloud suivent une stratégie cloud first

Gartner



Worldwide Cloud IT Infrastructure Market Forecast by Deployment Type, 2018 - 2024 (shres based on Value)

Source : IDC 2020

1 **Source :** *https://www.idc.com/getdoc.jsp?containerId=prUS46188120*

2. L'essor du multicloud

De plus en plus, les entreprises tiennent à ne pas confier tous leurs *workloads* et données à un seul fournisseur de cloud public. Ce qui explique qu'en 2020, plus de 90 % des entreprises internationales auront mis en place une stratégie multicloud selon IDC[2].

Pour Gartner, d'ici 2024, les stratégies multicloud vont permettre à deux tiers des entreprises de réduire leur dépendance envers un fournisseur donné[3]. Les principales motivations pour adopter le multicloud ne résident pas tant dans la recherche de la portabilité entre plateformes que dans des enjeux de *procurement*, de fonctionnalités et de réduction des risques. Ainsi, les entreprises tiennent à combiner plusieurs clouds publics pour améliorer leur résilience, optimiser leurs coûts et faire jouer la concurrence.

Le multicloud, conjugué aux stratégies cloud first, vient aiguiser le besoin d'accéder aux services de cloud public de façon fiable et efficace, au juste coût. La connectivité au cloud public ressort, là encore, comme un impératif stratégique pour les entreprises.

En 2020, plus de 90% des entreprises internationales auront mis en place une stratégie multicloud

IDC

3. Les datacenters de connectivité, véritables échangeurs de connexions au cloud public

Les datacenters de connectivité font figure de véritables hubs du numérique. Ils donnent accès à une densité sans pareille d'équipements réseaux, de fibres et d'interconnexions nationales permettant la collecte et la terminaison du trafic de toutes sources et origines.

Ils concentrent de plus un nombre inégalé d'opérateurs et de membres, dont les principaux fournisseurs de cloud public. D'où une proximité étroite avec ces fournisseurs en un même endroit, avec une possibilité d'interconnexion directe.

Ainsi, quelle que soit la nature d'interconnexion choisie – peering, interconnexion directe ou transit – l'entreprise a la certitude que tous ses interlocuteurs sont à distance de câble de son rack. Elle bénéficie ainsi d'un effet de *clustering* vertueux : plus un datacenter réunit d'acteurs, plus il y a d'interconnexions, plus les coûts baissent.

Aussi, les datacenters de connectivité offrent un environnement de prédilection pour garantir des connexions au cloud public fiables et performantes, propices aux stratégies cloud first et multicloud des entreprises, pour les entreprises.

2 **Source :** *https://www.idgconnect.com/document/01edcc81-015b-47fa-b32a-e1fd922bcb59/idc-futurescape-worldwide-cloud-2019-predictions*
3 **Source :** *https://www.gartner.com/smarterwithgartner/4-trends-impacting-cloud-adoption-in-2020/*

II. Les modèles de connexion au cloud public en datacenter de connectivité

Un datacenter de connectivité met à disposition des organisations trois types de connexion au cloud public : le cross connect, les liens managés et le peering – particulièrement le peering public.

Chacun de ces modes de connexion offre ses propres avantages. Pour parvenir à un choix avisé, une première étape semble incontournable : analyser avant tout les flux de trafic de l'entreprise et leur criticité. En effet, un mode de connexion au cloud public n'exclut pas les autres, et une même entreprise peut avoir recours à plusieurs d'entre eux. Or, c'est à la lumière de l'analyse de son trafic qu'une entreprise peut arbitrer quels sont les flux à orienter vers un cross connect, à confier à un spécialiste des liens managés, ou à écouler par le peering public.

1. Cross connect : en prise directe avec les opérateurs de cloud

L'avantage d'un datacenter de connectivité est de réunir en un même lieu les entreprises utilisatrices du cloud public et les opérateurs du domaine. Il est donc possible de mettre en place un câblage direct entre le routeur d'une entreprise et celui d'un opérateur cloud et d'assurer ainsi une connexion sans aucun intermédiaire.

Parmi les avantages de ce mode de connexion, citons d'abord le coût de la seule connexion – quelques dizaines d'euros par mois – qui fait du cross connect une solution imbattable en termes de dépense.

> ***« Parmi les atouts du cross connect : un coût de quelques euros par mois pour la connexion et un contrôle à 100 % des flux par l'entreprise »***
>
> ***Sami Slim** Deputy Sales Director, Telehouse France*

Sécurité : en cross connect, la sécurité est maximale puisque le flux est dédié à l'entreprise et contrôlé à 100 % par ses soins. De plus, en termes de disponibilité du service, le datacenter de connectivité va mettre en œuvre des accords de niveau de service, dont une disponibilité de service dépassant largement 99 % et des garanties de redondance qui limitent l'impact d'un éventuel incident.

Performance : le cross connect permet une connexion directe sans routeur intermédiaire entre celui de l'entreprise et celui de son fournisseur cloud, sans non plus passer par Internet. De plus, le datacenter de connectivité, principal interlocuteur de l'entreprise dans ce modèle, offre des options pour ajuster la bande passante aux besoins. À la clé, l'entreprise profite de performances maximales et d'un service très fiable.

Prérequis : l'entreprise doit disposer de son propre routeur et ouvrir un port chez le fournisseur de cloud public. Ses équipes doivent savoir choisir le bon port, le bon câble et configurer les flux. Ainsi, le cross connect nécessite une certaine maturité technique de la part de l'entreprise utilisatrice. Lorsque ces compétences ne sont pas présentes en interne, l'entreprise peut se tourner vers les équipes de son datacenter afin de se faire accompagner dans la démarche. Cette tactique leur permet d'accéder immédiatement aux compétences requises et de profiter de la maîtrise des coûts associée à l'externalisation (capex), par rapport à l'intégration en interne des compétences (opex).

Tendance : le cross connect représente autour de 15 % des connexions au cloud selon l'état des lieux chez Telehouse. On note une montée en force de ce type de connexion, les entreprises étant séduites par son faible coût, sa performance fiable et la maîtrise totale de la sécurité qu'elle apporte.

2. Liens managés : le prêt à l'emploi d'un intermédiaire expert

Avec Éric Desert, Ecosystem Sales Director – EMEA chez Megaport

Megaport

Dans des scénarios de multicloud devenus prioritaires, de nombreuses organisations cherchent à gérer facilement leur architecture d'entreprise et à l'adapter avec souplesse quand besoin est.

La solution NaaS – réseau en mode service – d'un fournisseur de liens managés répond particulièrement bien à ces cas d'usage. En effet, une solution NaaS est conçue sur le principe d'une connectivité au cloud sécurisée et à la demande vers un ou plusieurs fournisseurs. De plus, le NaaS met l'accent sur la simplicité d'usage.

Via la plateforme NaaS de Megaport, l'entreprise dispose d'un accès en ligne depuis lequel elle peut paramétrer sa connectivité en quelques minutes : il lui suffit de choisir le fournisseur cloud de son choix et de sélectionner un point d'accès au cloud parmi plus de 170 proposés (les « bretelles d'accès » au cloud ou « on-ramps »). À cela s'ajoute une bande passante évolutive qui permet d'adapter la consommation du réseau aux besoins de l'entreprise.

Les modalités d'engagement font également preuve de souplesse, puisqu'aucun contrat sur le long terme n'est requis. Une garantie de liberté pour l'entreprise qui évite ainsi tout effet de verrouillage auprès d'un fournisseur et peut composer un bouquet de services cloud selon ses priorités.

> ***« Une solution NaaS permet d'éviter la latence imprévisible de l'Internet, les restrictions de bande passante tout en profitant d'un réseau flexible et évolutif »***
>
> ***Éric Desert***
> *Ecosystem Sales Director*
> *EMEA chez Megaport*

Sécurité : dans ce modèle, la connexion privée est la seule qui vaille pour une sécurité maximale, à l'exemple du SDN (Software Defined Network) de Megaport entièrement exploité par la société. Les clients bénéficient d'une connectivité privée sur tout le réseau SDN en mode point à point ou aux « on-ramps » des fournisseurs cloud dans le monde entier, ce via la solution NaaS de leur prestataire respectif et en s'intégrant entièrement à leur API. Ainsi, en aucun point les données ne passent par Internet. L'entreprise peut utiliser ses propres méthodes de cryptage sur le réseau pour répondre aux exigences de ses charges de travail, sachant que le fournisseur de NaaS ne consulte pas et n'enregistre pas les données de ses clients.

Performance : la manière dont les entreprises se connectent aux ressources du cloud et aux autres datacenters joue un rôle essentiel dans les performances, la disponibilité et la simplicité d'usage des applications. De plus, il est essentiel de protéger les applications de production et stratégiques de toute interruption grâce à des architectures réseau résilientes et redondantes. Une solution NaaS permet d'éviter la latence imprévisible de l'Internet, les restrictions de bande passante tout en profitant d'un réseau flexible et évolutif.

Prérequis : pour accéder à la plateforme NaaS, les entreprises doivent ouvrir un port dans un datacenter compatible NaaS. Ce port peut ensuite être utilisé pour créer jusqu'à 100 connexions avec des fournisseurs de services ou d'autres datacenters. Lorsqu'une connectivité de cloud à cloud est requise, le déploiement d'un dispositif de routage virtuel permet d'éviter le recours à une infrastructure physique supplémentaire dans le datacenter.

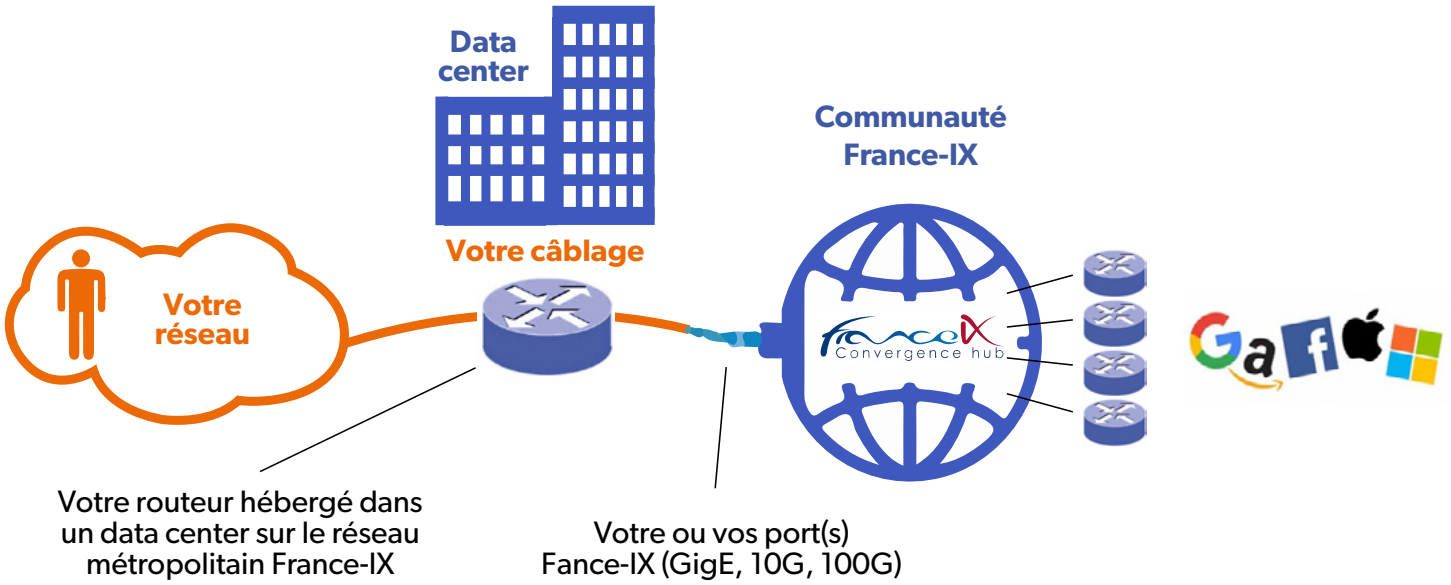
Tendance : les liens managés représentent un mode de connexion au cloud aujourd'hui plébiscité par près de 80 % des entreprises. Les liens managés bénéficient d'une offre très mature et bien identifiée par les entreprises utilisatrices, d'où sa prédominance actuelle comme mode d'accès aux services du cloud.

3. Peering : l'échange de flux de trafic avec les fournisseurs de cloud

Avec Simon Muyal, directeur technique de France-IX, point d'échange Internet

Le peering permet de procéder à un échange de trafic bilatéral en interconnectant les réseaux de chaque partie par l'intermédiaire d'un IXP (point d'échange Internet) présent dans le datacenter de connectivité, selon un accord de peering. Un IXP peut être illustré comme une multiprise de raccordement à un ensemble d'acteurs Internet – dont les fournisseurs de cloud public.

Le peering public, via l'Internet public, est particulièrement prisé parce qu'il permet une connexion directe, offrant une qualité de connexion optimale. Modèle ouvert et libre, il n'implique pas d'accord contractuel fort avec le fournisseur et permet une mise en service très rapide par activation d'une session BGP (Border Gateway Protocol), protocole d'échange de routes entre les AS (Autonomous Systems) du client et du fournisseur de cloud.



suite

3. Peering : l'échange de flux de trafic avec les fournisseurs de cloud

Avec Simon Muyal, directeur technique de France-IX, point d'échange Internet

Sécurité et résilience : la sécurité est pleinement intégrée dans l'infrastructure du point d'échange qui assure une résilience à tous les niveaux – infrastructure métropolitaine de fibres et routeurs. Il est également possible de recourir à un serveur de routes, facilitateur d'interconnexion, qui diminue le nombre de sessions BGP à configurer et se charge de vérifier la légitimité des routes, leurs origines et les bloque en cas d'anomalie. Le point d'échange met également à disposition des clients des mécanismes qui leur permettent de filtrer un DDoS en cas d'attaque. Enfin, l'utilisateur ne doit pas perdre de vue que le peering public lui permet de prolonger la sécurité en place dans sa propre infrastructure.

« Les corporates écoulent jusqu'à 80 % de leur volume de trafic sur un accès IXP peering public, pour accéder principalement à du contenu multicloud »

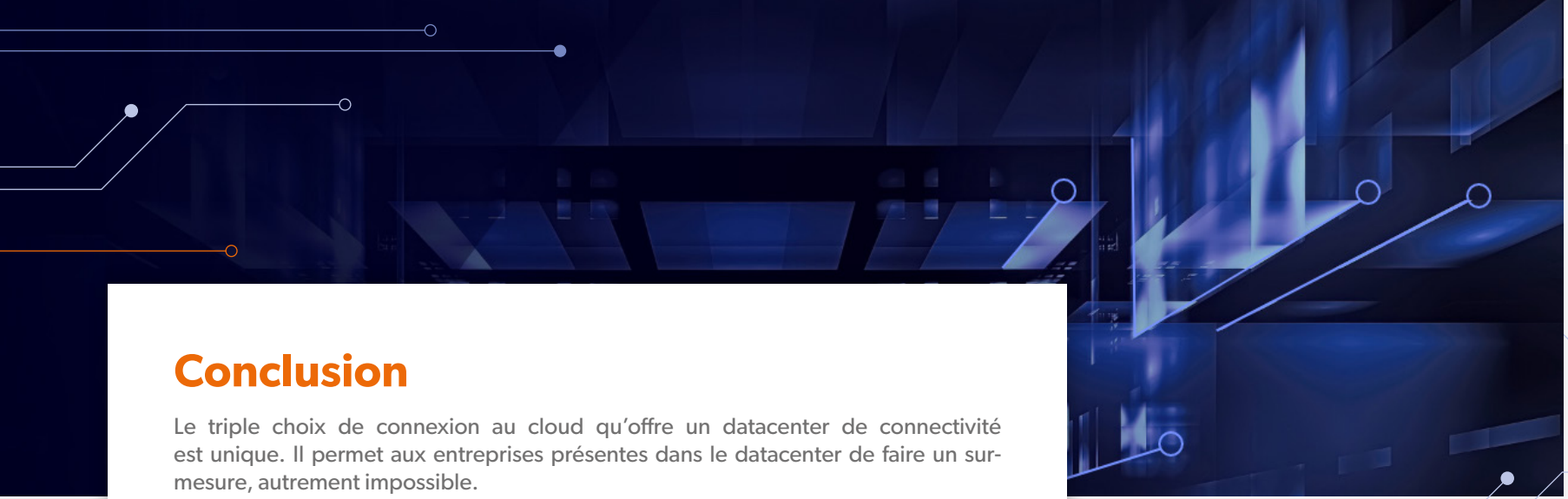
Simon Muyal
directeur technique de France-IX

Performance : le peering public offre des avantages de performance indéniables. Très simple à mettre en place par activation d'une session BGP, sans déploiement complexe de composants réseau, il permet de se raccorder et de passer en production rapidement. Il assure des délais d'acheminement de moins d'une milliseconde au sein du datacenter cœur de réseau où sont hébergés l'entreprise et ses fournisseurs cloud et ce, grâce à l'écosystème métropolitain du point d'échange sans déviation de longue distance, voire à l'étranger.

Prérequis : le peering public nécessite un numéro de système autonome et des adresses IP, dont les entreprises sont en général bien dotées. Autre impératif : héberger son infrastructure en datacenter – le cas de nombreuses entreprises – et y commander un cross connect vers l'infrastructure du point d'échange. Il est également possible d'atteindre le datacenter via des offres de transports Niveau 2. Le trafic est échangé via le routeur de l'entreprise situé dans le datacenter vers l'écosystème du point d'échange. L'ouverture de sessions BGP permet de recevoir une partie des routes d'Internet. Il en résulte un socle de connaissances BGP à bien maîtriser pour s'approprier les meilleures pratiques, notamment de configuration du port de peering. À ce sujet, une bonne pratique consiste à souscrire une capacité de trafic estimée modérée sur le port de peering, à suivre les statistiques et à faire évoluer l'abonnement (voire le port s'il est sous-dimensionné) une fois qu'une plus grande visibilité sur les flux à écouler se précise.

Le point d'échange peut toutefois proposer des services de peering managé et prendre ainsi la main sur ces paramètres à la demande du client. Quoi qu'il en soit, les entreprises sont souvent surprises de constater que le peering public écoule des flux plus importants que leurs estimations initiales, une bonne nouvelle en termes de maîtrise des coûts !

Tendance : si les fournisseurs de cloud sont de longue date connectés par peering, les entreprises l'abordent depuis plus récemment avec la montée en force de leur migration vers le cloud. Leur demande de peering est en hausse, d'autant plus quand elles suivent une stratégie multicloud. En effet, le peering offre la simplicité d'une prise unique d'échange de trafic point à point avec chacun des fournisseurs de cloud public, à des coûts maîtrisés.

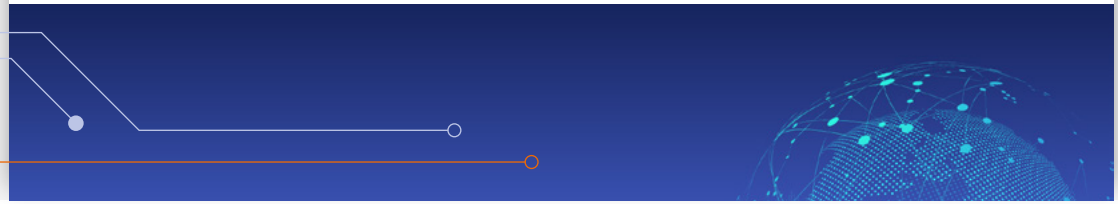


Conclusion

Le triple choix de connexion au cloud qu'offre un datacenter de connectivité est unique. Il permet aux entreprises présentes dans le datacenter de faire un sur-mesure, autrement impossible.

La nature du trafic d'une entreprise reste toujours la boussole en matière de choix de connexion au cloud, d'où l'étape préliminaire et essentielle d'analyse du type de trafic. Un autre point d'attention aide à parfaire la démarche : s'assurer que l'entreprise dispose des bonnes compétences réseau, tant pour préparer le terrain des connexions que pour les utiliser et les ajuster avec pertinence.

Certaines entreprises choisissent de muscler ces compétences réseau en interne. Pour les autres, l'opérateur du datacenter de connectivité reste un partenaire expert à qui confier la mission.



Remerciements :
*Ce livre blanc a été rédigé avec l'aide de Simon Muyal, directeur technique de **France-IX** et Éric Desert, Ecosystem Sales Director EMEA chez **Megaport**. Nous les remercions pour le partage de leur expertise et de leur vision des enjeux de connexion au cloud public.*

TELEHOUSE

A propos de Telehouse

Prestataire d'hébergement en Europe depuis 30 ans, Telehouse répond aux besoins d'hébergements physiques de plus de 3 000 entreprises de divers secteurs économiques tels que les télécoms, l'informatique, la finance, le luxe, l'automobile et l'énergie.

Disposant de plus de 40 Data centers dans le monde dont trois à Paris, Telehouse batit ses infrastructures et ses offres comme des réponses opérationnelles à vos besoisns en connectivité.

Telehouse est certifié ISO 14001, 50001, 9001, 27001 et PCI DSS (Chapitre 9 et 12).

TELEHOUSE France
137 boulevard Voltaire 75011 Paris
Tél: 0156064030
Email: colo@fr.telehouse.net
www.telehouse.fr