CLOUDFLARE

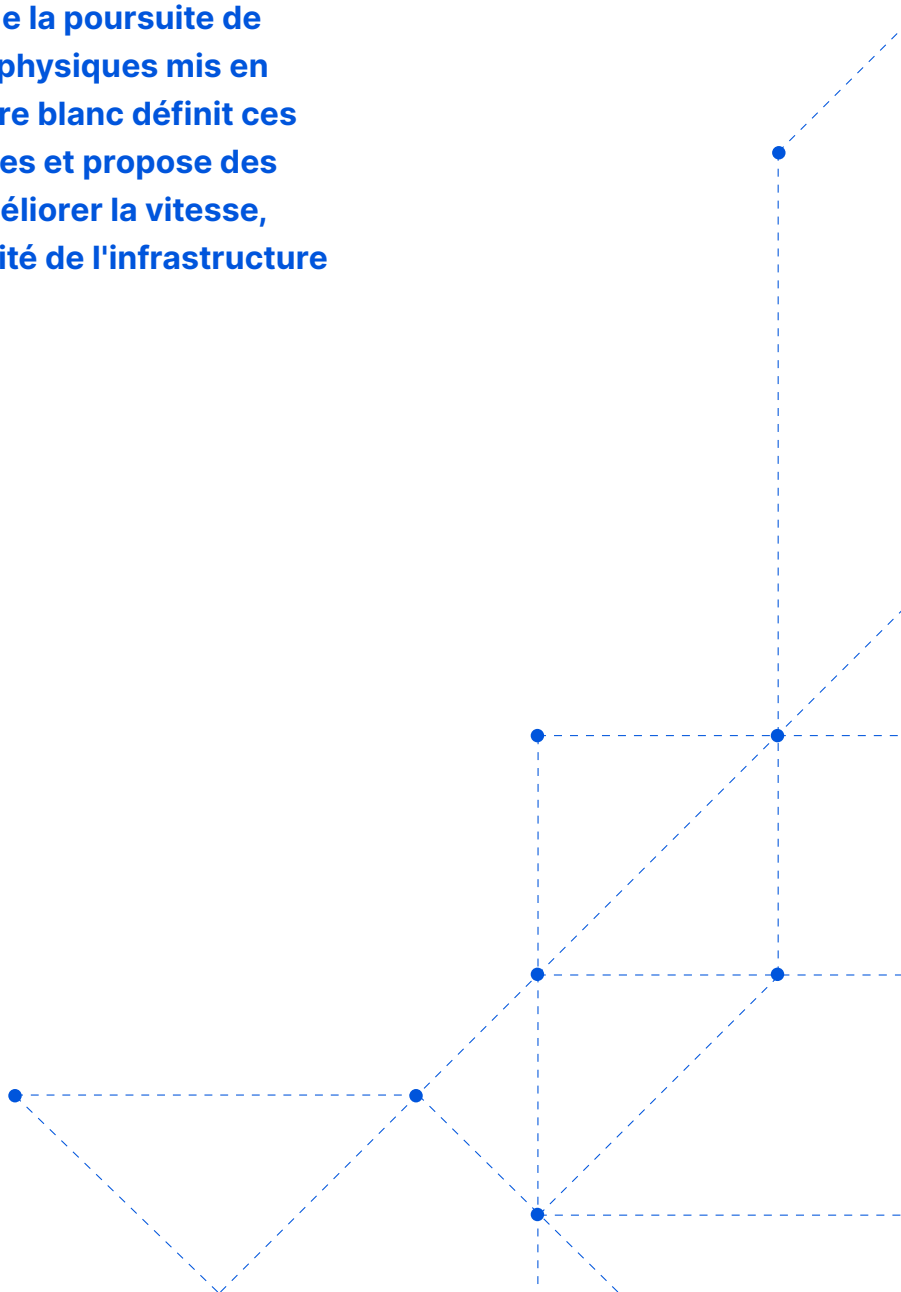
LIVRE BLANC

La fin des équipements réseau physiques

Pourquoi le moment est-il venu de vous défaire des équipements réseau ?

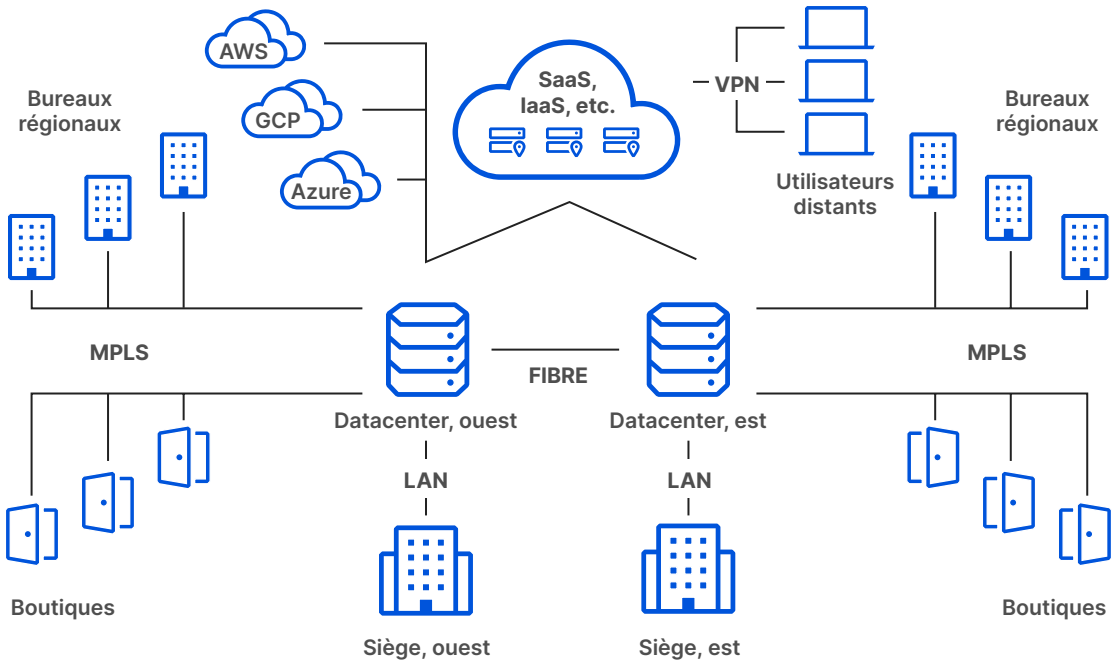
Synthèse

Si les fonctions de calcul et de stockage ont migré vers le cloud, de nombreuses fonctionnalités réseau demeurent sur site et engendrent diverses contraintes : limites de capacité, coût total de possession élevé, défis en matière de support technique et failles de sécurité. Alors que le travail hybride devient la norme, les entreprises connaissent des difficultés à garantir une capacité suffisante et une sécurité efficace. De nombreux projets de transformation ont stagné du fait de la poursuite de plans de déploiement d'équipements physiques mis en œuvre plus d'un an auparavant. Ce livre blanc définit ces problèmes, en évalue les conséquences et propose des solutions basées sur le cloud pour améliorer la vitesse, réduire les coûts et renforcer la sécurité de l'infrastructure cloud hybride.



Introduction

La stratégie de migration dans le cloud a déjà fait ses preuves en termes de réduction des coûts d'infrastructure, d'amélioration de la disponibilité des données et applications, ainsi que d'accroissement de l'agilité opérationnelle. Il est toutefois rare que cette migration s'effectue d'une seule traite. Nombre de grandes entreprises se retrouvent face à un mélange complexe d'éléments hébergés à la fois au sein d'une infrastructure multicloud et sur site :



Si ce type d'infrastructure hybride ne constitue pas nécessairement un mal, il entraîne néanmoins des complications. Pour être plus précis, il engendre des situations dans lesquelles différentes fonctions réseau (atténuation des attaques DDoS, équilibrage de charge, pare-feu, VPN, etc.) demeurent sur site.

Les équipements réseau traditionnels ne parviennent pas à sécuriser et accélérer de manière efficace une infrastructure essentielle au sein d'un monde axé sur le cloud. Cet amoncellement souvent désordonné d'appareils coûteux et reliés entre eux par un véritable imbroglio de câbles, à l'instar d'une toile d'araignée, s'est toujours révélé problématique. Si l'on ajoute le cloud à l'équation, des failles de sécurité apparaîtront rapidement, accompagnées d'une baisse des performances et de problèmes supplémentaires en matière de support technique.

Ce document décrit les risques et les écueils inhérents à la conservation d'équipements réseau physiques au sein d'un environnement en migration vers le cloud. Il propose également des stratégies permettant de développer un réseau plus sécurisé et plus efficace.

Les risques liés aux équipements physiques au sein d'un monde axé sur le cloud

Exploités de manière quelque peu différente selon les organisations, les équipements réseau physiques couvrent différentes fonctions spécifiques.

En voici quelques exemples courants :

Sécurité

- Protection contre les attaques DDoS
- Pare-feu
- Réseau privé virtuel (VPN)
- Politiques configurables

Performances et fiabilité

- Équilibrage de charge
- Accélération du trafic/ Optimisation WAN
- Filtrage des paquets
- Analyses du trafic

Lorsque ces équipements sont déployés sur site, l'architecture qui en résulte fait généralement face à cinq catégories de risques : **contraintes sur la chaîne d'approvisionnement, limites de capacité, coût total de possession élevé, défis en matière de support technique** et **failles de sécurités**.

Les trois premières catégories ont toujours été source de défis, même pour les équipes réseau et sécurité les plus aguerries. Les deux autres sont exacerbées par la migration vers le cloud.

Tensions sur la chaîne d'approvisionnement

À l'instar de n'importe quel produit physique, les équipements réseau physiques sont vulnérables aux diverses tensions pesant sur la chaîne d'approvisionnement. Lorsque les coûts du matériel augmentent, que certains matériaux ou composants se montrent plus problématiques à obtenir ou que les expéditeurs se retrouvent surchargés, l'achat ou le remplacement des équipements réseau se révèle plus difficile.

Malheureusement, ces difficultés (résultant d'ailleurs en grande partie des effets de la pandémie de COVID-19) s'avèrent monnaie courante ces derniers temps. D'après les recherches de Gartner, « les délais d'approvisionnement de 4 à 6 semaines étaient courants avant la pandémie. Désormais, ces délais atteignent souvent les 200 à 300 jours et certains clients ont même signalé des délais supérieurs à 430 jours. »

L'allongement de ces délais découle de plusieurs facteurs :

- **Difficultés logistiques :** les paradigmes traditionnels en matière de chaînes d'approvisionnement présentent de nombreux points de défaillance, comme le strict minimum en termes d'effectifs et une lourde dépendance envers des technologies plus ou moins sécurisées, soit autant d'écueils qui se sont récemment retournés contre ces modèles. La pandémie a provoqué la fermeture de nombreuses usines. Les entreprises de transport connaissent donc des retards et de nombreux types d'employés de la chaîne d'approvisionnement deviennent de plus en plus difficiles à recruter et à retenir. Mises bout à bout, toutes ces difficultés ont entraîné un allongement des délais de fabrication et d'approvisionnement des équipements physiques. L'aspect le plus complexe à retenir ici consiste à se souvenir que toute forme de logistique s'apparente à une course de relais. Le fait que votre entreprise ne connaisse pas de difficultés à un moment donné ne signifie pas qu'elle ne sera pas affectée par la rupture d'un maillon en amont de la chaîne d'approvisionnement.
- **Hausse du coût des matériaux :** les équipements réseau physiques reposent sur la disponibilité de diverses matières premières. En raison de la demande élevée et de l'offre limitée, les prix des matériaux ont ainsi connu une hausse vertigineuse. Les entreprises doivent non seulement attendre plus longtemps pour mettre la main sur les équipements dont elles ont besoin pour leur réseau, mais elles doivent également payer plus cher pour les obtenir. Face à de telles difficultés, Gartner s'attend malheureusement à ce que les délais d'approvisionnement des équipements physiques demeurent élevés jusqu'à début 2023 (source).

Tous ces défis ne resteront pas sans conséquence. En continuant à se focaliser sur l'approvisionnement, l'entretien et le remplacement des équipements physiques, les entreprises subissent des frais généraux plus élevés, consacrent plus de temps à la planification qu'à l'exécution et s'ajoutent des problèmes concernant la sécurisation de la chaîne d'approvisionnement physique dans une période d'incertitude. Plutôt que de se concentrer sur la logistique, les délais et le processus d'approvisionnement des équipements physiques, de même que sur le stockage de ces derniers, les entreprises devraient pouvoir se consacrer à la satisfaction des besoins de leurs clients.

Limites de capacité

De par leur nature même, il n'est pas surprenant que les équipements réseau physiques puissent être surchargés lors de pics de trafic inattendus, que le trafic soit ou non légitime. Toutefois, plusieurs tendances récentes ont révélé que ces limites constituaient une préoccupation plus courante.

Prenons l'exemple de l'atténuation des attaques DDoS (Distributed Denial of Service, déni de service distribué). La plus grande attaque DDoS de l'histoire s'est produite, d'après Microsoft, en novembre 2021 et aurait atteint un volume maximal de 3,47 Tb/s (source). Ces attaques DDoS se montreraient capables de surcharger largement les équipements physiques d'atténuation des attaques DDoS les plus avancés du marché, qui ne proposent généralement qu'une fraction de la capacité requise pour atténuer de telles attaques.

En novembre 2021, la plus grande attaque DDoS de l'histoire aurait atteint un volume maximal de 3,47 Tb/s.

Les entreprises n'attireront certes pas toutes des attaques d'une telle ampleur, mais elles ne disposent pas non plus de l'équipement d'atténuation DDoS le plus avancé. Un rapport Cloudflare révèle un accroissement des attaques volumétriques au cours du premier trimestre 2022. En réalité, les attaques supérieures à 10 Mp/s (millions de paquets par seconde) ont augmenté de plus de 300 % par rapport au trimestre précédent et les attaques dépassant les 100 Gb/s de 645 % (source). La forte hausse de ces attaques DDoS est non seulement alarmante, mais ces types d'attaques pourraient submerger de nombreuses solutions d'atténuation fondées sur des équipements physiques de haute capacité.

De surcroît, le volume des attaques ne prend pas en compte le trafic légitime susceptible de transiter par votre datacenter en même temps. Si une attaque de plus faible envergure venait à se produire pendant une période de trafic élevé (par exemple, lors du week-end du Black Friday, lorsque le nombre de pages vues quotidiennement sur les sites d'e-commerce double en moyenne du jour au lendemain (source), le pic de trafic pourrait s'avérer suffisamment important pour que les équipements de sécurité physiques arrivent au point de rupture.

L'atténuation des attaques DDoS ne représente qu'un exemple des limites de capacité des équipements physiques sur site.

En voici d'autres :

Équilibreurs de charge : les équilibreurs de charge individuels sur site peuvent facilement se retrouver surchargés par les pics soudains de trafic légitime. Lorsqu'une telle situation se produit, le processus d'acquisition et d'installation d'équipements physiques supplémentaires peut demander beaucoup de temps. La solution alternative consiste à maintenir une capacité suffisante pour faire face aux scénarios les plus pessimistes, mais cette approche nécessite de la part de l'entreprise qu'elle utilise en permanence de nombreux équipements physiques, pour un coût élevé donc.

VPN : le recours aux VPN (Virtual Private Networks, réseaux privés virtuels) est de plus en plus difficile à anticiper. Le passage au télétravail total et à une organisation du travail hybride constitue la nouvelle norme pour de nombreuses entreprises. Toutefois, l'approche traditionnelle par VPN ne saurait souffrir d'un manque de planification, d'entretien ou de gestion dans la mesure où les VPN n'ont jamais été conçus pour être utilisés en permanence ni par l'intégralité d'une entreprise. Lorsqu'un nombre trop important de collaborateurs se servent de ces solutions, la connectivité et la fiabilité de ces dernières en pâtissent. De même, la nature de la conception des VPN (c'est-à-dire, sans le moindre contrôle Zero Trust) peut engendrer des problèmes de sécurité. De plus, les entreprises peuvent faire appel à la tunnellisation fractionnée (Split Tunnelling) en cas de surcharge du VPN. Le trafic à destination du web ne transite alors pas par le VPN, soit un cas de figure qui ne facilite ni le suivi ni la gestion de l'activité des collaborateurs sur Internet.

Face à ces complications, l'une des réactions consiste à acheter davantage de matériel, plus récent et de capacité supérieure, mais cette approche introduit bien d'autres difficultés.

Coûts de possession

Comme pour les limitations des capacités, le coût élevé des équipements physiques pour datacenters ne devrait surprendre personne. Le coût initial du matériel nécessaire pour obtenir une capacité d'atténuation des attaques DDoS d'environ 100 Gb/s peut, par exemple, atteindre une somme comprise entre 400 000 et 500 000 USD.

Ces coûts ne représentent en outre qu'une partie du coût total de possession de ces équipements physiques.

Les dépenses suivantes doivent être prises en compte :

- Coûts liés à l'équipe : l'achat, l'exploitation et l'entretien des équipements physiques nécessaires pour assurer la protection de chaque couche du modèle OSI (et assurer le niveau de performances et de fiabilité attendu des sites web et des applications Internet modernes) exigent le déploiement d'experts de chacune de ces fonctions réseau au niveau de l'équipe. La mise en place d'une équipe présentant une expertise aussi étendue s'avère particulièrement coûteuse, en particulier dans le contexte actuel, marqué par un marché du travail plus tendu que jamais. Une étude de l'ISACA menée en 2022 a révélé que sur les 2 000 spécialistes de la cybersécurité qui ont pris part à l'enquête annuelle, 63 % déclarent que leur entreprise dispose de postes en cybersécurité non pourvus, c'est-à-dire 8 % de plus que l'année dernière (source).
- Coûts d'entretien : la durée de vie des équipements physiques installés sur site ne dépasse pas les 3 à 5 ans en moyenne. Pourtant, les garanties couvrant l'ensemble de cette période sont souvent conditionnées à des frais supplémentaires. Si l'on prend en compte le rythme de l'innovation technologique, il semble inévitable que la durée de vie de ces équipements sur site continue de raccourcir. Le cas contraire implique la nécessité de réparations imprévues (et donc non budgétisées) auprès du fabricant d'origine ou d'un tiers. Les dysfonctionnements des équipements physiques peuvent également entraîner une interruption de service du datacenter, soit une opération coûtant en moyenne plus de 8 800 USD par minute (source).
- Coûts de remplacement : le remplacement d'un équipement physique tous les trois ans nécessite non seulement de la part des entreprises qu'elles amortissent leur investissement initial, mais qu'elles consacrent également des ressources à l'expédition et à l'installation du nouveau matériel. Toute tentative de repousser ces remplacements l'expose bien souvent à des dysfonctionnements plus fréquents, synonymes de coûts d'entretien supplémentaires.

Comparons ce modèle aux services réseau fournis dans le cloud. Une équipe plus flexible peut assurer leur fonctionnement et ils n'imposent ni maintenance ni coûts d'expédition. De plus, ils n'obligent pas les organisations à faire un choix entre les mises à niveau coûteuses et l'augmentation des dysfonctionnements.

Les dysfonctionnements des équipements physiques peuvent entraîner une interruption de service du datacenter, soit une opération coûtant en moyenne plus de 8 800 USD par minute.

Défis en matière de support technique

En plus d'être coûteux, le support technique des équipements réseau physiques représente un défi logistique. Ces équipements nécessitent un déploiement fréquent de correctifs pour parer aux vulnérabilités et tactiques d'attaque les plus récentes. Or, il s'agit là d'un processus qui repose souvent sur une mise en œuvre manuelle, plus propice à l'erreur humaine.

Plus une entreprise utilise d'équipements physiques, plus elle risque de négliger un correctif par inattention ou par crainte d'affecter des systèmes essentiels. Lors d'un récent travail consultatif conjoint sur la cybersécurité, la National Security Agency (NSA), la Cybersecurity and Infrastructure Agency (CISA) et le Federal Bureau of Investigations (FBI) ont signalé l'exploitation de 16 failles publiquement connues des appareils réseau non mis à jour dans le cadre de campagnes de grande envergure (source). Ces actions d'exploitation ont touché différents appareils sur site, depuis les routeurs des PME jusqu'aux VPN des grandes entreprises. De même, elles ont potentiellement offert aux acteurs malveillants la possibilité de manipuler le trafic réseau et d'exfiltrer des données provenant des réseaux cibles.

Même si la plupart de ces 16 failles ont été qualifiées de critiques, la mise au point de mesures de correction et de réparation n'est pas chose aisée. En réalité, le déploiement de correctifs sur les équipements physiques peut s'avérer si complexe qu'une catégorie entière de logiciels existe pour aider les entreprises à se tenir à jour (source).

Les conséquences liées au défaut de déploiement d'un seul correctif peuvent atteindre des proportions considérables. L'équipement reste non seulement vulnérable, mais la publication d'un correctif implique également que la vulnérabilité correspondante devient une cible privilégiée pour les pirates opportunistes. Dans le cas des services de sécurité reposant sur le cloud, en revanche, la correction des vulnérabilités et le déploiement des mises à jour s'effectuent automatiquement par défaut. Par ailleurs, en fonction de la vitesse du réseau du fournisseur de cloud, la propagation de ces mesures peut s'opérer en tout juste 30 secondes.

Voici d'autres défis liés à la maintenance des équipements physiques :

- **Dépannage :** dans un scénario n'impliquant que des équipements physiques, le dépannage contraint souvent les équipes informatiques à débrancher les équilibreurs de charge, les pare-feu et les autres appareils installés sur site, les uns après les autres, afin de déterminer l'origine du problème rencontré.

  Cette tâche pour le moins fastidieuse se révèle encore plus compliquée en cas d'utilisation concomitante de services cloud. Les entreprises qui s'appuient sur des équipements physiques gèrent souvent l'accès à ces services à l'aide d'un datacenter centralisé et de tous les équipements qui le composent. Si les employés ne peuvent accéder à un service donné, l'équipe informatique doit donc contrôler également cet emplacement supplémentaire pour diagnostiquer les problèmes. D'après un récent rapport signé Productiv, 56 % de l'ensemble des applications SaaS entrent dans la catégorie du Shadow IT (l'informatique fantôme, c'est-à-dire, les applications non approuvées ou non gérées, installées à l'insu de l'équipe informatique). L'ampleur et la portée du problème connaissent donc une augmentation rapide (source).
- **Maintenance physique :** lorsqu'un équipement matériel tombe en panne, une nouvelle tâche fastidieuse incombe à l'équipe informatique, qui se voit alors contrainte de débrancher physiquement l'équipement, de commander un produit de remplacement et de le réinstaller. Compte tenu de l'échelle de nombreuses entreprises mondiales, les équipements nécessitant une telle intervention pourraient en outre se situer à l'autre bout de la planète.

Failles de sécurité

Même si une organisation disposait des ressources nécessaires à l'acquisition et à la maintenance en continu d'équipements matériels de dernière génération sur site offrant la plus grande capacité possible, l'infrastructure qui en résulterait connaîtrait malgré tout des insuffisances critiques en matière de sécurité, en particulier dans un univers tendant vers le cloud.

Envisagez l'utilisation d'une solution de gestion des accès du personnel. Si un VPN matériel peut certes établir des tunnels chiffrés entre les appareils utilisés par les employés en télétravail et les applications hébergées dans un datacenter interne, il ne peut ni surveiller ni sécuriser l'activité des utilisateurs une fois ces tunnels établis.

Si l'appareil d'un collaborateur se retrouve compromis par un logiciel malveillant ou qu'une tentative de phishing (hameçonnage) parvient à compromettre les identifiants utilisés par un employé pour se connecter au VPN, le pirate peut exploiter cette porte d'entrée dans le VPN pour accéder à une grande variété d'informations sensibles. Les logiciels malveillants et le phishing continuent de présenter un risque grave et génèrent des gains monétaires considérables pour les auteurs d'attaques. Selon le FBI, les pertes liées à la cybercriminalité se sont élevées à 6,9 milliards de dollars en 2021. Dans le cas précis de la compromission du courrier électronique professionnel (BEC, Business Email Compromise), les pertes engendrées se chiffrent à 2,4 milliards (source).

Si l'appareil d'un collaborateur est compromis par un logiciel malveillant ou qu'un hameçonnage compromet les identifiants utilisés par un employé pour se connecter au VPN, le pirate pourrait exploiter cette porte d'entrée vers le VPN afin d'accéder à une large gamme d'informations sensibles.

Les services cloud et les applications SaaS compliquent encore la sécurité des infrastructures organisées autour d'équipements physiques. Dans un modèle cloud hybride, par exemple, une entreprise exploite une infrastructure combinant à la fois des éléments sur site et d'autres dans le cloud. L'entreprise ne peut tout simplement pas envoyer ses équipements de sécurité matériels à un fournisseur de services cloud. Si elle souhaite continuer à utiliser des équipements physiques sur site pour son propre datacenter, différentes parties de son infrastructure seront protégées de différentes façons. La visibilité des équipes de sécurité et leur capacité à contrôler les attaques entrantes s'avéreront donc réduites.

Les services cloud peuvent surmonter ces deux difficultés en unifiant les datacenters et les services cloud au sein d'une même couche définie par logiciel.

Une explication détaillée de cette approche dépasserait le cadre du présent document. Aussi, si vous souhaitez en savoir plus, nous vous recommandons donc de consulter les articles suivants :

- Qu'est-ce qu'un réseau Zero Trust ?
- Qu'est-ce que le modèle SASE (Secure Access Service Edge) ?

Avantages et inconvénients des services d'amélioration des performances et de la sécurité basés sur le cloud

La prestation de services réseau par l'intermédiaire du cloud permet d'éviter bon nombre de problèmes liés au matériel : tensions sur la chaîne d'approvisionnement (supply chain), limites de capacité, coûts, défis en matière de support technique et failles de sécurité.

- **Chaîne d'approvisionnement :** de nombreux fournisseurs de services réseau basés sur le cloud sont conçus pour s'accorder avec les architectures mondiales modernes. Les difficultés liées à la chaîne d'approvisionnement se font donc moins sentir.
- **Capacité :** de par la nature distribuée et définie par logiciel du cloud, les organisations peuvent facilement faire évoluer leur capacité à mesure que leur activité se développe.
- **Coût :** les frais supplémentaires liés aux équipements physiques s'avèrent soit inexistants, soit plus faciles à planifier. De plus, les services cloud sont généralement classés dans la catégorie des dépenses de fonctionnement, pas dans celle des immobilisations liées aux investissements. Ce classement permet ainsi à de nombreuses entreprises de bénéficier d'avantages en matière de fiscalité et de comptabilité.
- **Support technique :** les besoins en termes de logistique et de ressources sont gérés par le fournisseur de services. En outre, le déploiement automatique des mises à jour permet de s'assurer qu'aucun correctif ne sera oublié.
- **Sécurité :** les services réseau définis par logiciel peuvent unifier différentes infrastructures sous une même couche de protection.

Les services réseau dans le cloud présentent toutefois leurs propres risques en cas de déploiement irréfléchi :

Risques	Description
Latence	Certaines fonctions réseau fondées sur le cloud reposent sur des data-centers spécialisés, eux-mêmes basés sur le cloud, comme les centres de nettoyage (scrubbing centers) destinés à l'atténuation des attaques DDoS. La redirection du trafic vers ces datacenters peut ajouter une latence considérable en fonction de la distance qui sépare le trafic du serveur de destination. Ce problème s'aggrave lorsqu'une entreprise recourt à différents fournisseurs pour exécuter différentes fonctions réseau. La latence peut ainsi atteindre plusieurs centaines de millisecondes lorsque le trafic doit être acheminé d'un fournisseur à un autre.
Support technique	Le dépannage demeure problématique lorsqu'une organisation utilise différents fournisseurs pour exécuter différentes fonctions. Il peut s'avérer difficile de déterminer quel fournisseur est à l'origine de la saturation ou de la panne.
Coûts	Lorsqu'une organisation passe par différents fournisseurs pour exécuter différentes fonctions, le temps (et donc l'argent) nécessaire pour gérer ces dernières peut encore se révéler très élevé.

Pour éviter ces problèmes, vous pouvez adopter les stratégies suivantes :

- **Cherchez des fournisseurs travaillant à la fois avec des infrastructures cloud et sur site.**
  L'équipe informatique et l'équipe dédiée à la sécurité pourront ainsi mettre en place des mesures de contrôle cohérentes et surveiller le trafic mondial de manière centralisée. La mise en place d'une architecture plus résiliente (c'est-à-dire, une architecture au sein de laquelle vos équipes peuvent se réorienter rapidement en fonction des fluctuations du marché) peut également vous aider.
- **Cherchez des fournisseurs de cloud proposant plusieurs fonctions réseau compatibles les unes avec les autres.**
  Ce type d'offre permettra bien souvent de réduire le nombre de sauts réseau que le trafic doit effectuer. Les utilisateurs finaux bénéficieront ainsi d'une réduction de la latence et donc d'une expérience utilisateur améliorée. Le dépannage des problèmes réseau se révèle également plus simple lorsque vous ne disposez que d'un seul prestataire à contacter. Enfin, le regroupement de plusieurs fonctions permet souvent de réduire les coûts.
- **Cherchez des fournisseurs de cloud capables d'assurer plusieurs fonctions réseau depuis chaque point de leur réseau.**
  Les fournisseurs qui étendent leur portefeuille de services par le biais d'acquisitions n'intègrent pas toujours pleinement ces nouveaux services. Certaines fonctions peuvent ainsi n'être proposées que par l'intermédiaire de certains datacenters. Afin d'éviter les problèmes mentionnés ci-dessus, recherchez des fournisseurs qui proposent ces fonctions sur l'ensemble de leur réseau.
- **Cherchez des fournisseurs cloud disposant d'une large présence mondiale.**
  Cette stratégie vient renforcer la précédente, afin de s'assurer que les utilisateurs finaux se situent toujours à proximité du réseau, où qu'ils se trouvent. Elle crée également une vaste surface réseau permettant d'absorber le trafic des attaques DDoS et d'exécuter d'autres fonctions réseau nécessitant une grande capacité.

Ce que Cloudflare peut vous apporter

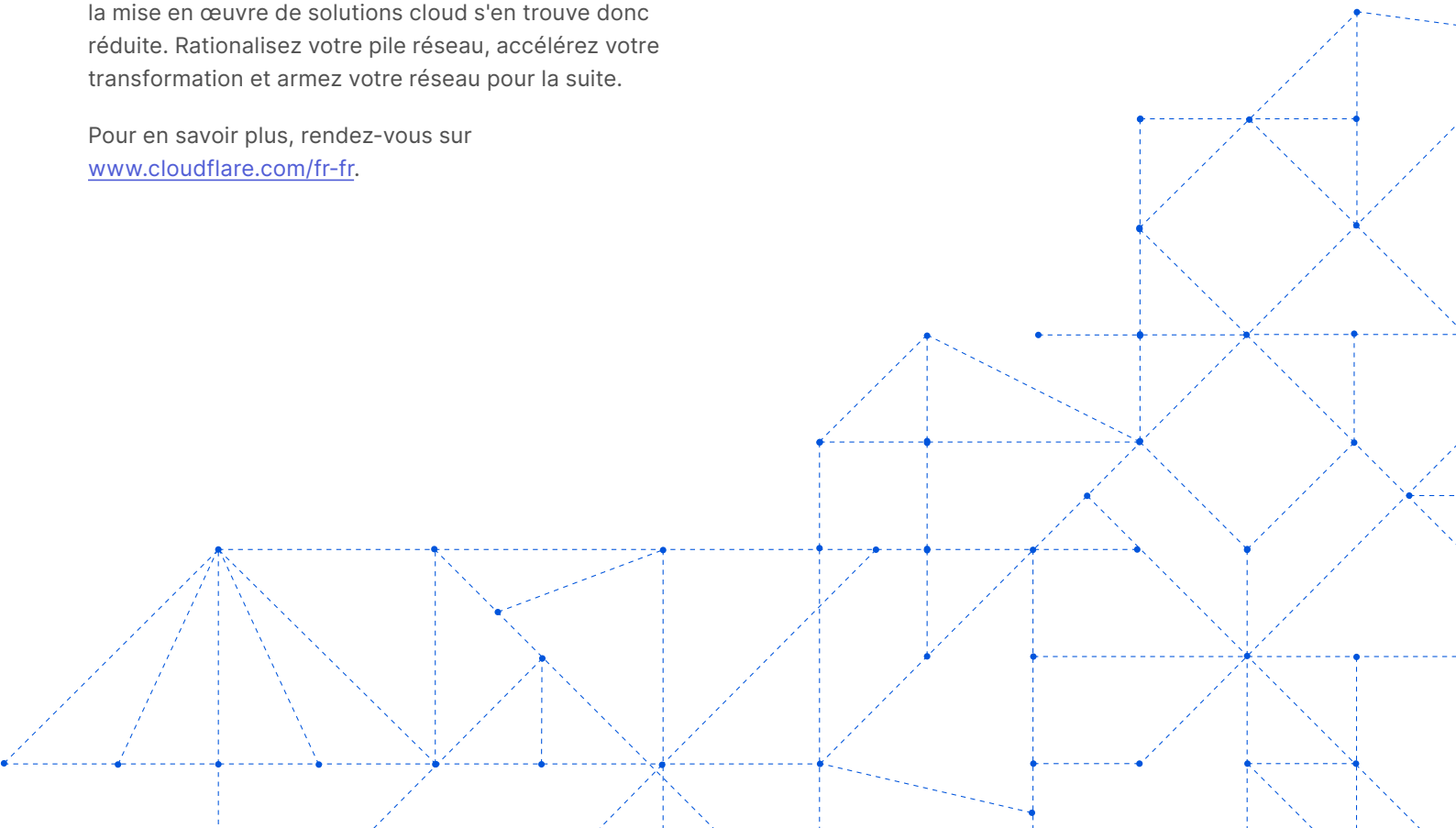
Comment les entreprises peuvent-elles accélérer la transformation de leur réseau, sans avoir à attendre l'arrivée de matériel ni engloutir plus d'argent dans des équipements qui ne dureront que quelques années ? Grâce à Cloudflare.

Cloudflare a développé une plate-forme cloud mondiale offrant un vaste éventail de services. Cette dernière permet de mieux sécuriser les organisations, d'améliorer les performances de leurs applications et d'éliminer la complexité et les coûts liés à la gestion de chaque élément physique d'un réseau. Cette plate-forme sert de plan de contrôle unifié, facile à utiliser et évolutif permettant d'assurer la sécurité, les performances et la fiabilité de l'ensemble des applications sur site, hybrides, cloud et SaaS (Software-as-a-Service, logiciel en tant que service).

Détail essentiel du réseau mondial de Cloudflare (qui s'étend sur plus de 270 villes à travers le monde) : chaque datacenter qui le compose peut assurer chacun de ces services. La latence susceptible de compliquer la mise en œuvre de solutions cloud s'en trouve donc réduite. Rationalisez votre pile réseau, accélérez votre transformation et armez votre réseau pour la suite.

Pour en savoir plus, rendez-vous sur www.cloudflare.com/fr-fr.

> « Dropbox est récemment devenue une entreprise qui accorde la priorité au virtuel. Nous avons étudié l'incidence de cette stratégie commerciale sur notre approche de la sécurité et notre architecture réseau. Nous apprécions la manière dont Cloudflare nous soutient et nous aide, ainsi que d'autres entreprises comme la nôtre, pleinement axées sur le télétravail, à découvrir comment s'adapter à cette « nouvelle norme ». »
>
> Konstantin Sinichkin
> **Responsable de l'ingénierie chez Dropbox**



+33 7 57 90 52 73 | enterprise@cloudflare.com | www.cloudflare.com/fr-fr/

RÉV : BDES-3313.2022JUN10