Livre blanc

Surmonter les défis du réseau multicloud : optimiser l'expérience liée aux applications et aux charges de travail

Sponsorisé par : Cisco

Brad Casemore
Avril 2021

LE POINT DE VUE D'IDC

Quelles que soient leur taille et leurs activités, les entreprises poursuivent leur transformation numérique afin de renforcer leur agilité, leur efficacité et leur compétitivité, tout en adoptant des systèmes IT hybrides et multicloud pour parvenir à leurs fins. Par conséquent, les applications et charges de travail autrefois centralisées dans des environnements de datacenter sur site sont redistribuées dans différents clouds. En parallèle, le personnel est de plus en plus mobile et dispersé dans des campus, des sites annexes et, de plus en plus souvent, à domicile en conséquence de la pandémie de COVID-19. Il en résulte de nouvelles contraintes pour le datacenter traditionnel, ainsi que l'obligation pour les entreprises de moderniser et d'étendre leur infrastructure réseau afin de pouvoir prendre en charge des applications multicloud distribuées, tout en offrant un accès sécurisé depuis un nombre sans précédent d'emplacements et de points périphériques du réseau.

Les réseaux multicloud doivent être capables de fournir l'agilité, la flexibilité, les capacités de mise à l'échelle élastique, l'efficacité opérationnelle et le niveau de sécurité dont ont besoin les entreprises qui ont de plus en plus recours au cloud.

Dans les environnements multicloud, le réseau occupe une place essentielle, comme jamais auparavant. La migration des applications et des charges de travail vers les IaaS et les SaaS du cloud public nécessite d'avoir recours à une infrastructure réseau multicloud étendue et fiable – depuis les charges de travail jusqu'aux accès – capable de fournir l'agilité, la flexibilité, les capacités de mise à l'échelle élastique, l'efficacité opérationnelle et le niveau de sécurité dont ont besoin les entreprises qui ont de plus en plus recours au cloud.

Ce livre blanc se penche sur le besoin d'un réseau multicloud étendu capable de répondre à toutes les exigences des applications cloud IaaS et SaaS, ainsi qu'à la demande d'un accès permanent, réactif et sécurisé aux applications cloud.

VUE D'ENSEMBLE DE LA SITUATION

Avant même la pandémie de COVID-19, les entreprises ont commencé à utiliser de multiples clouds pour atteindre leurs objectifs de transformation numérique. Bien que la plupart des entreprises exécutent encore certaines applications stratégiques dans des environnements installés sur site, elles ont opté pour des solutions SaaS pour certains cas d'usage appropriés, et un nombre croissant d'entre

elles ont transféré des applications, nouvelles ou anciennes, vers des IaaS et des PaaS du cloud (par exemple, AWS, Microsoft Azure, Google Cloud et IBM Cloud).

Les entreprises qui avaient déjà commencé cette migration vers le cloud en accélèrent la cadence, tandis que celles qui hésitaient changent d'avis rapidement. Le réseau du datacenter, ainsi que le réseau étendu (WAN) qui englobe de multiples clouds, sites annexes et emplacement périphériques doivent nécessairement évoluer étant donné que les besoins d'agilité et de résilience des activités deviennent des objectifs à long terme.

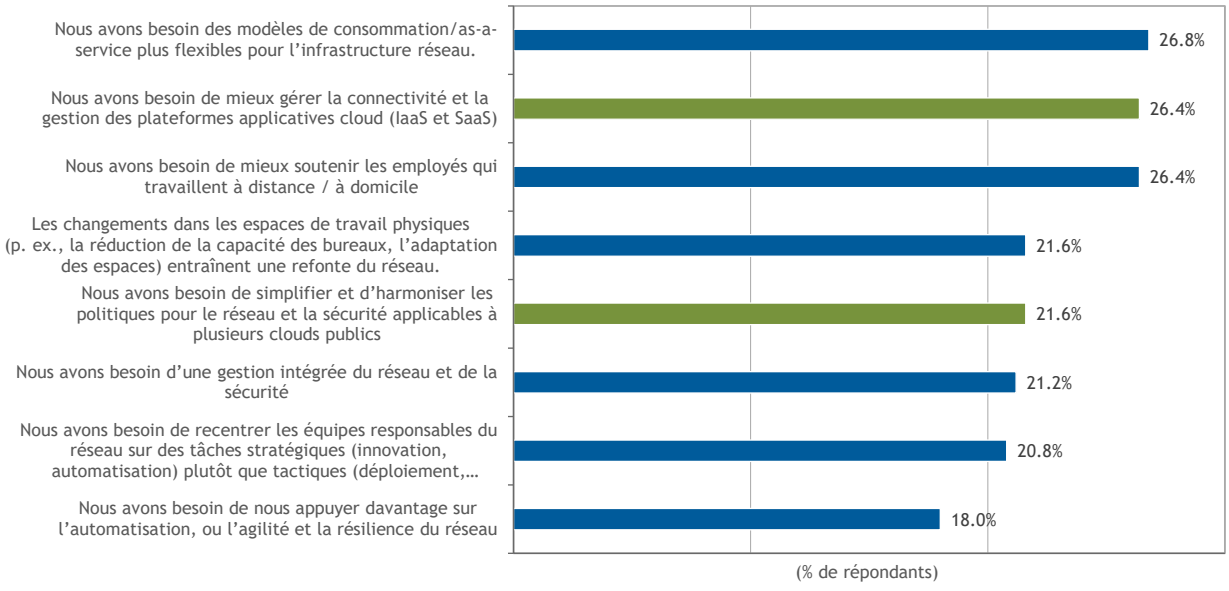
La modernisation du réseau pour les environnements multicloud repose sur un principe de base : l'application distribuée est le nouveau centre de gravité. À l'ère du multicloud, qui n'aurait pas vu le jour sans une automatisation toujours plus poussée, les réseaux doivent plus que jamais concorder avec les besoins dynamiques des applications et des charges de travail.

En effet, les leaders du domaine IT reconnaissent qu'il est nécessaire d'améliorer la connectivité réseau et la sécurité pour les applications cloud. Au cours d'une enquête récente d'IDC intitulée *Enterprise Networking: Emergence of the New Normal Survey,* les participants ont indiqué qu'une meilleur gestion de la connectivité des plateformes cloud (26,4 %) et la simplification des politiques pour le réseau et la sécurité dans de multiples clouds publics (21,6 %) figuraient parmi leurs principales priorités en 2021 (voir Figure 1).

FIGURE 1

Priorités inscrites dans les stratégies réseau en 2021 : consommation flexible, connectivité cloud et prise en charge des personnes travaillant à distance

Q. Quelles sont vos grandes priorités en matière de stratégie réseau pour 2021 ?



États-Unis ; n = 250

Source : *Enterprise Networking: Emergence of the New Normal Survey,* IDC, décembre 2020

À mesure que l'informatique hybride se généralise – avec des applications distribuées dans des environnements sur site et de cloud public – il est non seulement nécessaire de mettre en place une politique cohérente et extensible pour le réseau et la sécurité, mais aussi de prévoir de nouveaux moyens d'acheminer rapidement et efficacement le trafic entre les réseaux cloud locaux et centraux, en fournissant des points d'entrée sécurisés et des voies d'accès pratiques, afin de limiter les latences, d'améliorer la disponibilité et de fournir une expérience améliorée liée aux applications.

Le réseau multicloud est également une composante clé de la stratégie de l'entreprise en matière de résilience. Il doit être capable de détecter les menaces et les pannes, et d'y répondre rapidement, car celles-ci peuvent avoir un impact sur la disponibilité des applications et des services. Si la pandémie de COVID-19 a rappelé brutalement cette nécessité l'année dernière, d'autres événements imprévus peuvent survenir, et sont survenus, tels que l'incendie récent dans le datacenter du prestataire cloud OVH ayant entrainé des interruptions de services. Les résultats des dernières enquêtes d'IDC montrent que les entreprises subissent en moyenne deux interruptions de service cloud chaque année, et qu'elles estiment en restant prudentes que cela leur coûte en moyenne 250 000 dollars par heure

LES DEFIS LIES AU RESEAU MULTICLOUD POUR LES CHARGES DE TRAVAIL DISTRIBUEES

Compte tenu de la prolifération des applications et des microservices sur le réseau (qui englobe le datacenter, les services de cloud public, les services hébergés sur le réseau, ainsi que les environnements périphériques), le réseau du datacenter ne s'inscrit plus dans un périmètre géographique précis et ne se situe plus à un emplacement physique spécifique. Il est devenu une sorte de « réseau neural » qui interconnecte des « clusters neuraux » exécutés en parallèle des applications et des données.

Les entreprises veulent avoir la possibilité d'étendre leurs politiques, qui gouvernent les locataires et les applications, dans toutes les ramifications du réseau qui passent par les environnements sur site et cloud.

Toutefois, la mise en réseau de ces charges de travail, applications et microservices de plus en plus distribués est relativement complexe. Cette complexité se traduit notamment par la nécessité de provisionner manuellement les ressources, ce qui prend beaucoup de temps. Les difficultés liées au routage du trafic dans plusieurs zones géographiques et clouds, ainsi considérables que les disparités entre les différents clouds, concernant notamment le nombre de routes, la segmentation et le débit disponible – exigent une expertise pointue pour chaque API et service réseau cloud spécifique. Les dépendances des applications doivent également être prises en compte. En moyenne, chaque application compte quatre à huit dépendances applicatives, et ces dépendances seront de plus en plus nombreuses dans les années à venir.

En matière de réseau, la complexité se traduit toujours par des processus plus coûteux et longs. Outre les défis précédemment cités, les entreprises qui cherchent à s'appuyer sur un environnement multicloud constatent souvent qu'elles doivent surprovisionner les services de pare-feu et déployer un routage asymétrique tortueux pour s'adapter au pare-feu de chaque cloud. Elles ont également du mal à tirer parti des capacités offertes par le

cloud en termes de mise à l'échelle automatique et élastique, notamment lorsqu'il s'agit d'introduire des services réseau et de sécurité.

En effet, les entreprises veulent avoir la possibilité d'étendre leurs politiques, qui gouvernent les locataires et les applications, dans toutes les ramifications du réseau qui passent par les environnements sur site et cloud, en s'appuyant sur une gestion et un provisionnement centralisés des politiques pour l'ensemble de cet aspect critique de l'infrastructure réseau.

L'importance croissante accordée à la protection holistique des charges de travail

L'intégrité et la sécurité des charges de travail, indépendamment de leur emplacement et de leur architecture, restent au centre des préoccupations de toutes les entreprises. Il est donc essentiel que les mécanismes et modèles de sécurité modernes s'appliquent à toutes les applications traditionnelles et cloud natives, ces dernières étant axées sur les conteneurs et les microservices.

Aujourd'hui, les entreprises utilisent de nombreux produits spécifiques pour différents cas d'usage de protection des charges de travail. Elles ont tendance à utiliser des outils distincts pour leurs nombreux et différents besoins en matière de sécurité. De plus en plus, les entreprises qui souhaitent réduire les niveaux de complexité de la gestion des environnements multicloud, cherchent des moyens de consolider les outils qu'elles utilisent pour garantir une protection holistique de leurs charges de travail.

LES DÉFIS LIÉS AU RÉSEAU MULTICLOUD POUR LES ACCÈS SÉCURISÉS EN PÉRIPHÉRIE

En périphérie également, de nouvelles difficultés sont apparues pour les accès utilisateur, étant donné qu'une partie croissante des applications utilisées et consommées réside dans des environnements SaaS et IaaS du cloud public aux dépens des datacenters sur site. Les départements IT sont contraints de s'appuyer sur de multiples approches compliquées et chronophages afin de garantir une expérience utilisateur cohérente et sécurisée pour chaque service cloud (p. ex., AWS, Microsoft Azure et Office 365, Google Cloud et Salesforce).

Dans ce contexte, le SD-WAN a émergé afin de répondre aux besoins d'accès aux charges de travail IaaS et SaaS soumises à différentes contraintes réseau : bande passante adéquate, faible niveau de latence (surtout pour les applications collaboratives), pertes et réordonnancement de paquets, jitter.

Au cours de l'enquête d'IDC conduite en 2019 et intitulée *Software-Defined WAN (SD-WAN) Survey*, 73 % des entreprises interrogées ont indiqué que les services SaaS et cloud pesaient considérablement dans leur choix d'une technologie WAN, et ce pourcentage atteint plus de 78 % si l'on tient compte des répondants ayant affirmé qu'ils reconsidéreront cette question au cours des 12 à 24 prochains mois. De plus, seulement 4 % d'entre elles ont indiqué qu'elles n'avaient aucune connexion WAN avec un quelconque prestataire IaaS.

Compte tenu des progrès réalisés en matière d'informatique hybride et de multicloud, les équipes IT cherchent des moyens simples de connecter les sites à de multiples clouds. Elles souhaitent également disposer de capacités

Pour les accès aux charges de travail et applications IaaS et SaaS, un SD-WAN capable de prendre en charge des environnements multicloud doit offrir des capacités d'automatisation intent-based (basée sur les objectifs de l'entreprise) afin de fournir aux administrateurs réseau les moyens nécessaires leur permettant de proposer la meilleure expérience liée aux applications.

télémétriques et d'une bonne visibilité permettant d'obtenir des informations exploitables qui les aideront à affiner les politiques déclaratives basées sur les applications, et à accélérer les dépannages, ainsi que l'identification et la résolution des problèmes liés aux applications et aux réseaux.

Pour les accès aux charges de travail IaaS et aux applications SaaS, un SD-WAN capable de prendre en charge des environnements multicloud doit offrir des capacités d'automatisation intent-based (basée sur les objectifs de l'entreprise) afin de fournir aux administrateurs réseau les moyens nécessaires leur permettant de proposer la meilleure expérience liée aux applications. Un SD-WAN capable de prendre en charge le multicloud doit permettre une sélection dynamique et optimale des chemins, une intégration avec les services cloud et des optimisations lorsque des applications cloud souffrent d'une latence élevée ou de jitter.

L'importance d'un accès sécurisé aux environnements multicloud

Un cadre efficace visant à sécuriser les accès aux environnements multicloud doit permettre de combiner le réseau et la sécurité en périphérie d'une part, et les capacités de sécurité du cloud d'autre part pour garantir une protection cohérente des utilisateurs et des données, quel que soit leur emplacement. Le personnel est plus dispersé que jamais, mais quel que soit le lieu où travaillent les employés, ils ont besoin de pouvoir accéder au réseau en toute sécurité et de profiter de la meilleure expérience possible pour toutes les applications et charges de travail sur site, SaaS ou IaaS. Malheureusement, les anciennes architectures de sécurité et la profusion d'outils disparates ne le permettent pas et, en conséquence, les utilisateurs et les entreprises restent vulnérables.

Les équipes responsables du réseau et de la sécurité reconnaissent de plus en plus souvent qu'elles ont besoin de s'appuyer sur une approche à la fois holistique et simple qui englobe les fonctions réseau et de sécurité pour garantir un accès sécurisé aux environnements multicloud.

COMMENT ABORDER LE RÉSEAU MULTICLOUD

Lorsqu'une entreprise élabore une stratégie multicloud dans le cadre de ses initiatives de transformation numérique, il est essentiel qu'elle adopte une approche exhaustive et progressive du réseau multicloud si elle souhaite voir ses projets aboutir et lui procurer les avantages, ainsi que les gains d'efficacité opérationnelle attendus.

Après avoir évalué ses applications distribuées, ainsi que ses objectifs immédiats et à plus long terme en matière de cloud, le réseau multicloud pourra être abordé en mettant l'accent sur deux principaux aspects :

- **Les charges de travail distribuées :** les charges de travail, y compris celles reposant sur une architecture moderne composée de microservices et de conteneurs, doivent être interconnectées au moyen d'un réseau agile, flexible et disposant de capacités de mise à l'échelle élastique permettant de simplifier et de rationaliser le provisionnement, la gestion et la sécurité.
- **L'accès sécurisé :** un accès aux applications (sur site, IaaS et SaaS) hautement disponible et réactif est essentiel, et doit s'accompagner d'une protection, d'une fiabilité et de performances solides, quel que soit l'endroit où se trouvent les utilisateurs et les appareils.

Comment aborder le réseau multicloud pour les charges de travail distribuées

1. **Une visibilité sur le réseau et des capacités analytiques étendues.** Les applications étant distribuées au-delà du datacenter de l'entreprise, les équipes IT ont besoin d'une télémétrie, d'une visibilité et de capacités analytiques étendues à l'ensemble du datacenter, du WAN, du réseau haut débit et des réseaux cloud.
2. **Automatisation basée sur les politiques étendue à tout le réseau.** Les outils d'automatisation réseau doivent permettre aux équipes NetOps d'étendre et d'appliquer des politiques cohérentes aux environnements IaaS et de limiter la complexité croissante de la gestion des charges de travail distribuées dans différents environnements cloud.
3. **Protection des charges de travail et des données contre les attaques.** Les entreprises doivent avoir une visibilité globale en temps réel qui les aidera à identifier/répondre aux menaces et anomalies auxquelles sont exposés les utilisateurs, les appareils, les applications, les charges de travail et les processus (workflows).
4. **Association d'outils dédiés à l'automatisation et à l'extraction d'informations afin de créer un réseau intent-based (IBN) en boucle fermée.** L'association de l'automatisation basée sur les politiques et des informations obtenues grâce à l'IA dans un modèle IBN en boucle fermée peut permettre d'automatiser l'ensemble de la gestion du réseau.

Comment aborder le réseau multicloud pour les accès sécurisés

1. **Déploiement d'un SD-WAN sécurisé.** Les équipes IT ont intérêt à déployer une architecture SD-WAN simple et sécurisée pour simplifier et automatiser la connectivité des sites annexes qui bénéficieront alors de tous les services nécessaires et d'une connectivité dynamique leur permettant de s'adapter aux contraintes du travail mobile et à l'utilisation croissante d'applications SaaS et IaaS. Un tel SD-WAN apportera suffisamment de cohérence pour pouvoir exploiter n'importe quel réseau cloud sur la base des mêmes mécanismes que ceux habituellement utilisés par l'entreprise IT.

Optimisation du SD-WAN pour améliorer les performances et la sécurité des SaaS et IaaS. Le SD-WAN doit permettre de sélectionner automatiquement et dynamiquement le chemin le plus rapide et le plus fiable vers les applications SaaS, grâce à une gestion du trafic en temps réel qui garantira une expérience optimale aux utilisateurs. De la même manière, le SD-WAN doit permettre une connexion automatisée, simple et sécurisée aux environnements IaaS, tels qu'AWS et Azure. Une console de gestion centralisée permettra aux équipes opérationnelles et celles responsables du réseau d'automatiser les connexions des clouds privés aux environnements IaaS.

2. **Une sécurité basée sur le cloud pour un accès sécurisé permanent.** Dès lors que les charges de travail et les données sont transférées hors site, une plateforme unique cloud native peut permettre de consolider et de faire converger l'ensemble des capacités de sécurité et réseau qui étaient auparavant fournies par de multiples produits spécifiques cloisonnés. Cela permet à la fois de sécuriser complètement les accès des utilisateurs, quel que soit l'endroit où ils se trouvent, et de réduire les coûts opérationnels.
3. **La colocation pour agréger et accélérer les connexions cloud.** Le SD-WAN permet aux architectures distribuées d'avoir recours à des installations en colocation afin de réduire le nombre de points de sorties cloud, de régionaliser la sécurité pour limiter les surfaces d'attaque et d'optimiser l'efficacité du réseau.

LA MODERNISATION DU RÉSEAU MULTICLOUD SELON CISCO

Cisco travaille en étroite collaboration avec les départements IT des entreprises pour les aider à accélérer et à simplifier leur passage au cloud à l'aide d'une large gamme de solutions technologiques et de services de réseau multicloud, et d'un vaste écosystème de partenaires facilitant notamment les intégrations avec les principaux prestataires cloud.

Dans son approche du réseau multicloud, Cisco met l'accent sur la gestion des applications distribuées, ainsi que sur la sécurisation et la fiabilité des accès à ces applications. Pour ces deux aspects, l'intent-based networking (IBN) joue un rôle central visant à fournir les capacités d'automatisation, les informations essentielles et le niveau de sécurité requis dans des environnements multicloud de plus en plus complexes.

Le réseau multicloud de Cisco pour les charges de travail distribuées

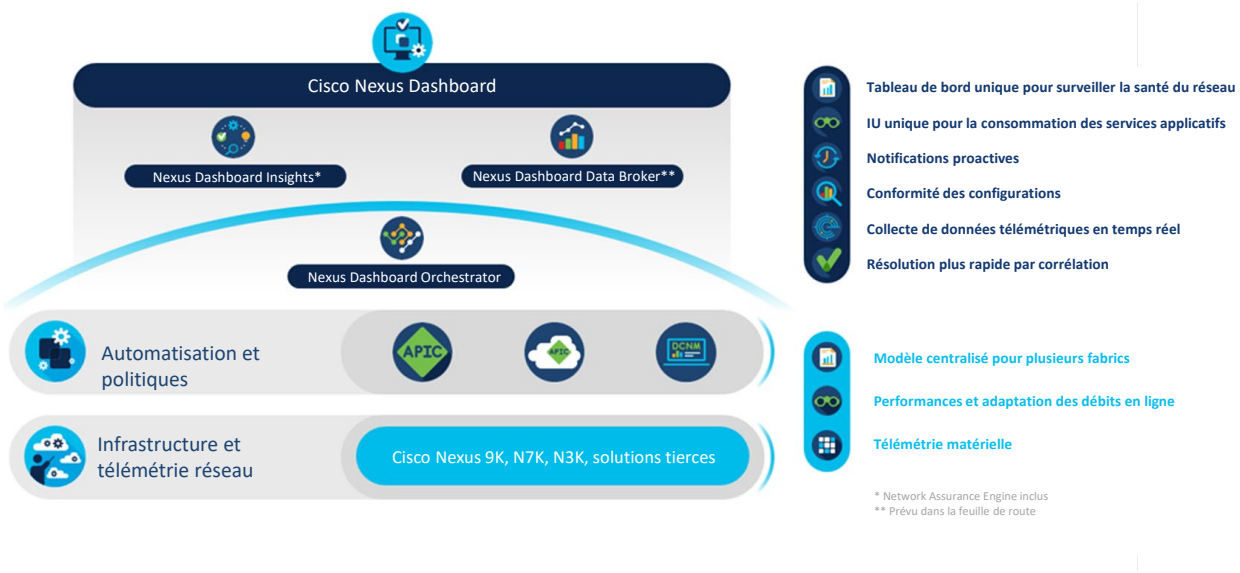
L'approche retenue par Cisco en matière d'informatique hybride et de multicloud aide les architectes cloud et réseau à élaborer des modèles opératoires cohérents et simplifiés couvrant les datacenters sur site, le cloud public et les environnements périphériques. Elle a été développée en vue de simplifier la gestion des réseaux multicloud intrinsèquement complexes en s'appuyant notamment sur des opérations réseau assistées par IA.

Opérations unifiées sur le réseau multicloud

La plateforme **Cisco Nexus Dashboard Platform** permet de gérer les opérations de manière unifiée et proactive, tout en s'appuyant sur des informations exploitables sur l'ensemble du datacenter et des réseaux multicloud. Elle peut permettre de réduire les niveaux de complexité opérationnelle grâce à l'intégration uniforme des datacenters, et des services opérationnels de Cisco et d'autres partenaires. Cisco Nexus Dashboard Insights, Cisco Nexus Dashboard Orchestrator, Cisco Nexus Dashboard Data Broker et d'autres applications tierces peuvent être regroupées au sein d'un tableau de bord unique (voir figure 2).

FIGURE 2

Gamme de solutions réseau multicloud de Cisco pour les charges de travail distribuées



Source : Cisco, 2021

Automatisation du réseau pour les charges de travail multicloud

Cisco ACI est une solution logicielle intent-based pour les réseaux de datacenter ; elle est conçue pour une gestion agile des applications et une automatisation multicloud sécurisée.

Cisco Data Center Network Manager (DCNM) est une plateforme de gestion pour tous les déploiements sous Cisco NX-OS, depuis les nouvelles architectures fabric jusqu'aux réseaux de stockage, dans les environnements sur site et cloud.

Sécurisation du datacenter multicloud

Cisco Secure Data Center associe Cisco ACI, Cisco Firepower Next-Generation Firewall, Cisco Stealthwatch et Cisco Tetration pour sécuriser les environnements modernes de datacenter et cloud.

Réseau multicloud pour les accès

Réseaux étendus aux environnements SaaS et IaaS

Cisco SD-WAN Cloud OnRamp offre des fonctionnalités avancées et rationalisées de connectivité à un ou plusieurs clouds (IaaS et SaaS), directement depuis un site annexe, et via Internet, un fournisseur de solutions d'interconnexion ou même des environnements en colocation. Le SD-WAN offre aux utilisateurs les mêmes niveaux de sécurité et de performance pour les applications, dans le cloud et dans les environnements sur site.

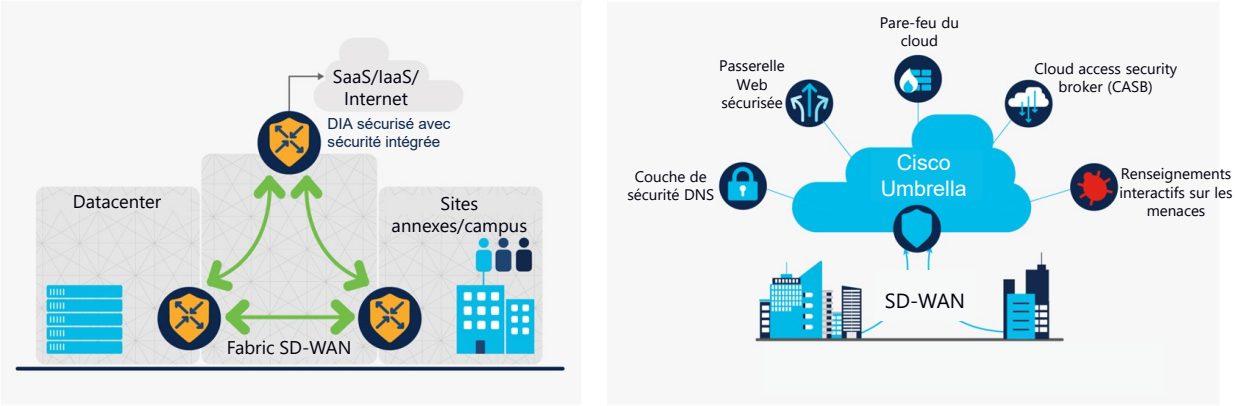
Sécurisation des accès multicloud

Cisco SD-WAN Security réunit des fonctionnalités avancées pour la gestion du réseau et la sécurité afin de sécuriser toutes les couches de la pile sur la plateforme SD-WAN et dans le cloud. Cette approche intégrée de la sécurité du SD-WAN offre une sécurité avancée contre les menaces à tous les niveaux – depuis les sites annexes qui se connectent à de multiples Saas ou IaaS cloud, jusqu'au datencer et tout système connecté à Internet.

Cisco SD-WAN with Cisco Umbrella fournit une protection contre les menaces et une visibilité permettant de se prémunir contre les attaques lancées via le Web. Grâce au cloud Cisco Umbrella, les entreprises bénéficient d'une meilleure visibilité et d'un contrôle renforcé sur les applications SaaS et Internet (voir figure 3).

FIGURE 3

Le SD-WAN et les solutions de sécurité au niveau des points d'accès (SASE) de Cisco offrent de multiples options de sécurisation des accès pour les réseaux multicloud



Sécurité intégrée sur site

Sécurité cloud et SASE

Source : Cisco, 2021

Sécurité cloud et cadre SASE de Cisco

Le cadre SASE regroupe des composantes du SD-WAN, des mécanismes de sécurité basés sur le cloud ainsi qu'un modèle de sécurité « zero trust ».

- **Cisco Umbrella** est un service de sécurité cloud qui unifie une multitude de fonctions de sécurité afin d'aider les entreprises de toute taille à profiter de l'accès direct à Internet (DIA), à sécuriser les applications cloud, et à étendre leur protection aux utilisateurs nomades et aux sites annexes.
- **Cisco Duo** est une plateforme de sécurité zero trust orientée utilisateur permettant d'assurer la protection de tous les utilisateurs, tous les appareils et toutes les applications. Le système d'authentification multifacteur (MFA) de Cisco Duo permet de contrôler l'identité de tous les utilisateurs, où qu'ils se trouvent, avant d'autoriser les accès aux applications sur site et cloud.

DÉFIS ET OPPORTUNITÉS

La modernisation et la transformation des réseaux d'entreprise pour le multicloud offre des perspectives uniques pour les fournisseurs de solutions et leurs clients. En modernisant le réseau depuis l'infrastructure centrale jusqu'à la périphérie pour s'adapter aux applications modernes, à l'informatique hybride et aux environnements multicloud, les entreprises seront davantage en mesure de fournir l'agilité, la flexibilité, les capacités de mise à l'échelle élastique, la fiabilité et les niveaux de sécurité dont ont besoin les environnements applicatifs distribués. Il en résultera une accélération de la mise sur le marché des produits et des services, une résilience renforcée, une efficacité améliorée des IT en général, un provisionnement, des dépannages et une résolution des problèmes plus rapides, ainsi qu'une meilleure efficacité/réactivité des accès aux applications pour les utilisateurs qui bénéficieront ainsi d'une expérience numérique améliorée.

Les entreprises qui cherchent à moderniser leur réseau pour les environnements multicloud sont confrontées à un défi majeur consistant à bien appréhender leurs environnements applicatifs actuels et futurs, y compris les projets de déploiement d'applications dans le cloud public (IaaS et SaaS). En outre, elles doivent s'assurer que les aspects opérationnels IT, y compris les équipes responsables du réseau, soient parfaitement en phase avec les fonctions métiers et les développeurs pour veiller à ce que l'infrastructure concorde avec les objectifs stratégiques de l'entreprise, ainsi qu'avec les besoins des développeurs et les exigences des applications.

Pour Cisco, le principal défi consistera à s'assurer que son portefeuille de solutions de réseau multicloud continue à s'adapter et à répondre aux exigences en constante évolution de l'informatique hybride et des environnements multicloud grâce aux fonctionnalités étendues de ses produits, notamment pour la télémétrie, la visibilité sur le réseau et la prise en charge complète de multiples clouds publics. Cisco peut encore optimiser l'expérience applicative multicloud offerte à ses clients en intégrant ses solutions de réseau multicloud avec ses capacités d'observabilité sur l'ensemble de la pile. Cisco doit également veiller à ce que ses produits répondent mieux aux besoins de ses clients que les solutions proposées par ses anciens et nouveaux concurrents, y compris les fournisseurs de solutions SDN et IBN, les startups spécialisées dans les solutions de réseau multicloud et les prestataires cloud IaaS.

CONCLUSION

Les impératifs de la transformation numérique et le recours croissant au multicloud redéfinissent les frontières du datacenter, ainsi que les exigences du réseau pour le datacenter et la périphérie où se connectent les utilisateurs pour accéder et utiliser les applications. En effet, les applications et les charges de travail, qui constituent le moteur numérique de l'entreprise moderne, sont désormais distribuées et hébergées non seulement dans le datacenter sur site, mais également dans de multiples clouds publics. Cette évolution a des répercussions sur le placement des charges de travail, le trafic et les exigences liées aux accès depuis les sites annexes, les campus et même les environnements de travail à domicile.

Bien que la gestion des environnements multicloud soit complexe et qu'il soit difficile d'en extraire le plein potentiel, un réseau multicloud modernisé conçu pour s'adapter et fournir des charges de travail distribuées peut réduire de façon importante ce niveau de complexité et contribuer au succès des stratégies multicloud et des initiatives de transformation numériques.

L'intent-based networking, qui s'appuie sur des objectifs déclarés et des processus réseau en boucle fermée, peut simplifier un tel réseau multicloud en permettant aux administrateurs réseau et aux architectes cloud de gérer le réseau de manière proactive, de garantir la disponibilité et la fiabilité du réseau, tout en mettant en place une sécurité zero trust à tous les niveaux du réseau multicloud.

Si les architectes réseau et cloud parviennent à élaborer et mettre en œuvre une feuille de route stratégique en faisant concorder l'infrastructure réseau avec les stratégies applicatives et multicloud, ils seront capables d'apporter l'agilité, la flexibilité, l'évolutivité et la sécurité nécessaires aux charges de travail distribuées, et permettront ainsi à leur entreprise d'en tirer des bénéfices sans précédent.

Si les architectes réseau et cloud parviennent à élaborer et mettre en œuvre une feuille de route stratégique faisant concorder l'infrastructure réseau avec les stratégies applicatives et multicloud, ils seront capables d'apporter l'agilité, la flexibilité, l'évolutivité et la sécurité nécessaires aux charges de travail distribuées, et permettront ainsi à leur entreprise d'en tirer des bénéfices sans précédent.

MESSAGE DU SPONSOR

Les solutions intent-basesd networking de Cisco aident les entreprises à atteindre leurs objectifs dans les environnements multicloud, tels que la gestion d'applications distribuées dans de multiples clouds et l'optimisation de l'expérience utilisateur.

Les solutions de Cisco pour le réseau multicloud aident les équipes IT à garantir la connectivité, la sécurité et l'application de politiques cohérentes dans tous les clouds afin d'en simplifier la gestion. Grâce à des modèles de consommation flexibles, à un écosystème large et diversifié, et à des innovations visant à simplifier les opérations et à réduire les risques, le département IT peut étendre le datacenter à tous les endroits où circulent les données et fournir aux utilisateurs un accès sécurisé là où ils en ont besoin.

Pour en savoir plus sur la gamme de produits de Cisco, rendez vous sur
http://www.cisco.com/go/multicloudnetworking

À propos d'IDC

IDC est un acteur majeur de la recherche, du conseil et de l'événementiel sur les marchés des technologies de l'information, des télécommunications et des technologies grand public. IDC aide les professionnels évoluant sur les marchés IT et les investisseurs à prendre des décisions stratégiques basées sur des données factuelles. Plus de 1 100 analystes d'IDC proposent leur expertise globale, régionale et locale sur les opportunités et les tendances technologies dans plus de 110 pays à travers le monde. Depuis plus de 50 ans, IDC propose des analyses stratégiques pour aider ses clients à atteindre leurs objectifs clés. IDC est une filiale de la société IDG, leader mondial du marché de l'information dédiée aux technologies de l'information.

Siège social mondial :

140 Kendrick Street
Building B
Needham, MA 02494, États-Unis
États-Unis
+1.508.872.8200
Twitter : @IDC
blogs.idc.com
www.idc.com