

**Que rechercher dans une  
solution Secure SD-WAN  
pour environnements  
multi-cloud**

# Table des matières

<b>Synthèse</b> .....	<b>3</b>
<b>Les raisons d'une adoption rapide du multi-cloud</b> .....	<b>5</b>
<b>Plus de clouds, plus de complexité</b> .....	<b>5</b>
<b>Des clouds multiples exigent une sécurité et une gestion unifiées</b> .....	<b>7</b>
<b>Que rechercher dans une solution SD-WAN</b> .....	<b>9</b>
<b>Une solution SD-WAN efficace simplifie le multi-cloud</b> .....	<b>11</b>

## Synthèse

Le cloud mobilise une part toujours plus importante des budgets des DSI, au point que certaines entreprises font appel à de nombreux environnements cloud différents pour bâtir leur infrastructure informatique. Un modèle multi-cloud implique de choisir plusieurs services de cloud pour définir des fonctions spécifiques. Aujourd'hui, les entreprises ont presque toutes adopté la flexibilité que leur apporte le multi-cloud : 93 % d'entre elles ont actuellement une stratégie multi-cloud en place.<sup>1</sup> Cependant, l'interconnexion entre les instances présentes sur différents clouds et le edge WAN des datacenters est source de complexité dans le déploiement, de performances réseau aléatoires et d'une inflation des coûts de connectivité.

Le SD-WAN (software-defined wide-area networking) favorise l'adoption du multi-cloud tout en simplifiant l'infrastructure WAN et en réduisant les coûts de connectivité. Mais pour être efficace, le SD-WAN doit être sécurisé.



**Les prévisions de croissance du marché mondial de l'IaaS (Infrastructure-as-a-Service) s'établissent à un taux de croissance annuel composé (TCAC) de près de 28 %, pour un marché estimé à 101,56 milliards de dollars à l'horizon 2023.<sup>2</sup>**

## Les raisons d'une adoption rapide du multi-cloud

Une stratégie multi-cloud évite aux entreprises toute dépendance exclusive vis-à-vis d'un fournisseur et permet de sélectionner les services de cloud les mieux adaptées à une application ou une instance particulière. Le multi-cloud se différencie du cloud hybride qui associe clouds publics et privés pour optimiser les performances, la sécurité et la flexibilité. Le multi-cloud signifie simplement que les entreprises ont la possibilité de choisir le meilleur fournisseur de cloud pour chacun de leurs besoins en matière d'infrastructures et d'applications.

Les organisations peuvent choisir des services économiques et exploiter des clouds géographiquement disséminés dans une optique de reprise sur sinistre, de respect des exigences de souveraineté des données et d'expérience utilisateur renforcée.

Le modèle multi-cloud offre également une redondance, idéale en cas d'indisponibilité opérationnelle. Bien que les dysfonctionnements soient plus rares chez les fournisseurs de services, une telle perturbation reste néanmoins

possible. Alors que les entreprises continuent à migrer des instances de plus en plus critiques vers le cloud, une panne ou une dégradation des performances peut sérieusement affecter la continuité de leurs opérations métier et la qualité globale de l'expérience proposée.

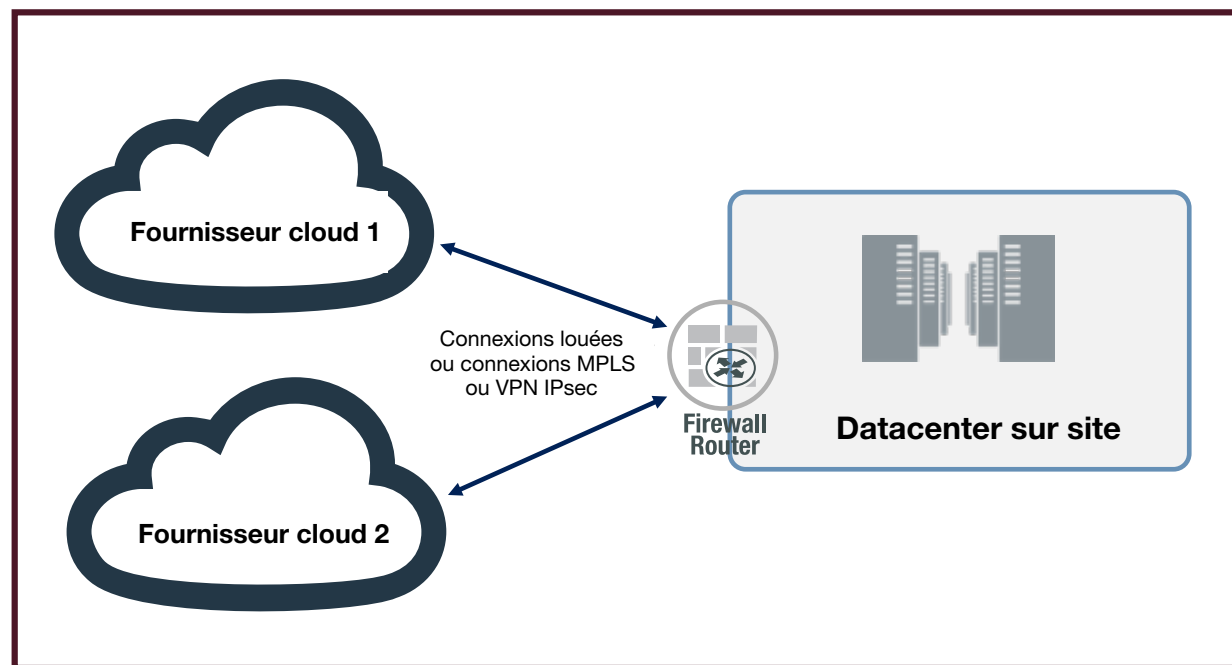
## Plus de clouds, plus de complexité

Malgré ses innombrables avantages, le multi-cloud alimente la complexité en matière d'administration, en particulier si de nouveaux services de cloud sont adoptés de manière ad-hoc, plutôt que d'être planifiés en amont.<sup>3</sup> Cette complexité est à l'origine de défis de gestion et opérationnels, en matière de déploiement, de performances réseau et de coûts d'exploitation. Peu d'équipes informatiques ont l'expertise nécessaire pour gérer un environnement mixte, constitué d'environnements de cloud public, de cloud privé et sur site, une situation exacerbée par la pénurie constante de compétences IT et de cybersécurité. Les entreprises dont les ressources sont limitées auront du mal à suivre.

Pour assurer un contrôle et une visibilité centralisés au sein des topologies réseau en étoile, le trafic applicatif de chaque cloud est généralement réacheminé des fournisseurs vers un datacenter sur site via des rétroliens MPLS (Multiprotocol Label Switching) coûteux. Cette pratique renchérit les coûts opérationnels et peut ralentir l'expérience des utilisateurs des applications, en raison de congestions liées à la sécurité.

**Alors que les entreprises ne cessent de recourir toujours plus au cloud pour héberger leurs applications, un accès direct et performant est essentiel.<sup>4</sup>**

De plus, celles qui ne disposent pas de capacités centralisées de gestion et de monitoring, ne pourront appliquer leur règles de sécurité de manière uniforme sur tous leurs environnements cloud. C'est une visibilité de bout en bout sur l'infrastructure qui fait défaut aux entreprises, aboutissant à des risques d'intrusion, de pertes de données ou de pénalités pour raisons de non-conformité. Heureusement, il existe une architecture différente pour répondre à ces problématiques.



- Environnement complexe
- Performances applicatives dégradées
- Coûts de connexion élevés

Schéma 1 : Environnements multi-cloud actuels.

# Des clouds multiples exigent une sécurité et une gestion unifiées

Pour optimiser les avantages et la flexibilité d'une stratégie multi-cloud, les technologies de sécurité et de réseau doivent offrir les avantages suivants :

- Utiliser des connexions optimales pour acheminer le trafic applicatif de manière fiable et performante
- Tirer parti de connexions Internet à haut débit afin de réduire les coûts
- Bénéficier d'une visibilité sur l'ensemble de votre infrastructure réseau
- Équilibrer la répartition des instances et de leurs charges entre clouds publics et privés
- Mettre en œuvre des politiques réseau et de sécurité cohérentes sur les différents clouds

Compte tenu de ses fonctionnalités d'automatisation et de sa dimension stratégique, le SD-WAN est devenu la solution de choix pour faire évoluer rapidement les réseaux cloud et le multi-cloud.<sup>5</sup> Le SD-WAN permet aux entreprises de compléter ou de remplacer les connexions MPLS coûteuses par des options de connectivité via Internet plus économiques, adaptées aux applications. Ceci compense la dégradation des performances, une problématique qui s'accroît compte tenu du volume de trafic provenant des applications cloud utilisées dans l'entreprise.

**Les applications hébergées dans le cloud public peuvent utiliser des passerelles SD-WAN avancées, basées sur le cloud, pour diriger le trafic entre ces applications.<sup>6</sup>**

# Que rechercher dans une solution SD-WAN

Les solutions SD-WAN varient considérablement en termes de fonctionnalités. Les entreprises doivent examiner attentivement tous les coûts associés, qu'il s'agisse des investissements initiaux (CapEx) ou des charges d'exploitation (OpEx), ainsi que les besoins en matière de gestion, de performances et, surtout, de sécurité.

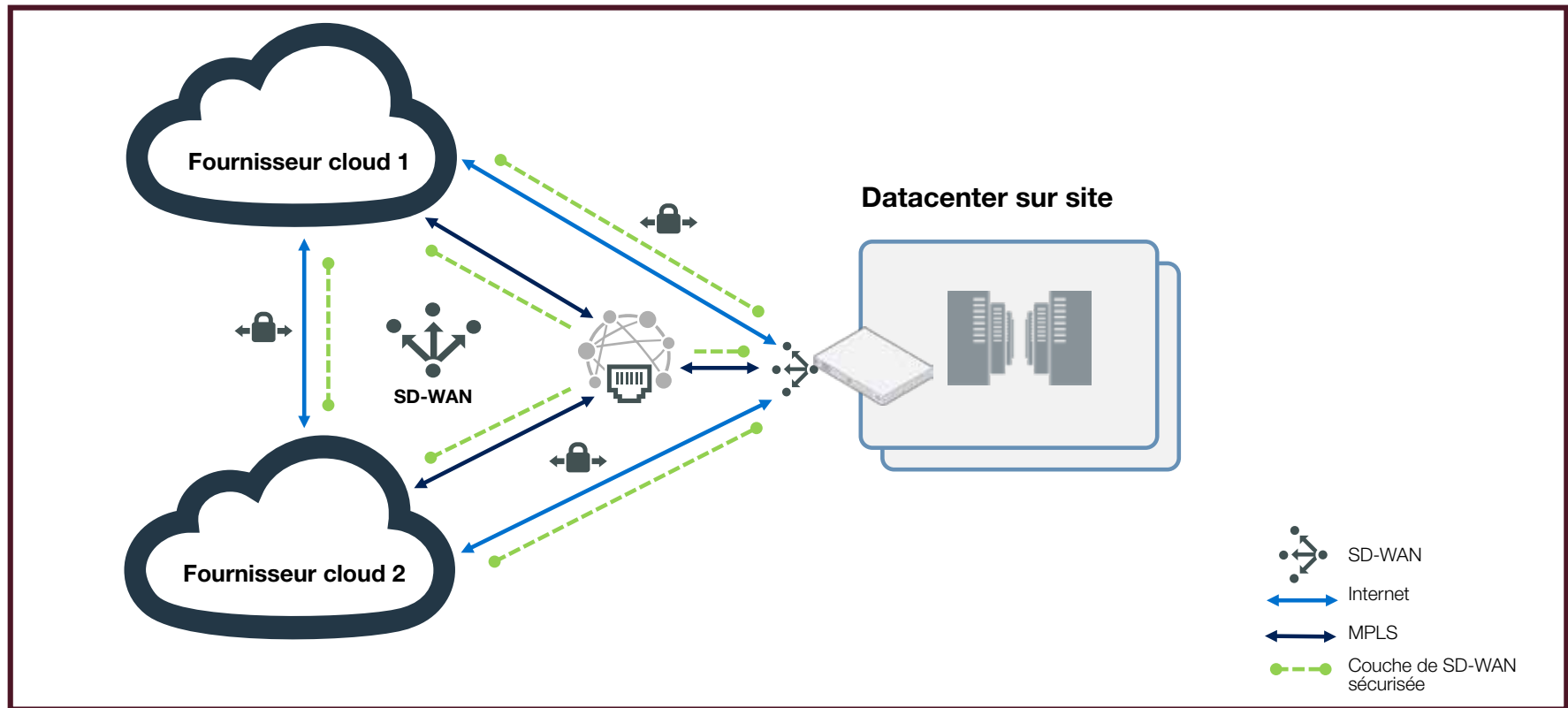


Schéma 2 : Interconnexion de plusieurs clouds sur SD-WAN.



- **Un SD-WAN consolidé et sécurisé.** Une approche décentralisée au SD-WAN implique d'investir dans plusieurs dispositifs pour fournir toutes les fonctionnalités réseau et de sécurité nécessaires à une solution fonctionnelle. Cette approche cloisonnée induit des failles de sécurité qui ne demandent qu'à être exploitées lors des cyberattaques. Une solution unique, associant fonctionnalités SD-WAN avancées et pare-feu de nouvelle génération (Next-Generation Firewall, NGFW) peut cependant pallier ces lacunes de sécurité et alléger les investissements initiaux (CapEx).
- **Simplifier le déploiement et la gestion.** Le SD-WAN décentralisé diminue également les coûts d'exploitation, compte tenu de l'investissement en temps des équipes pour déployer, orchestrer et gérer la solution. Une solution SD-WAN consolidée centralise ces processus. Une interface commune à partir d'**une console unique** simplifie les opérations et allège la charge des équipes dont le personnel est limité. Privilégiez une solution offrant des **intégrations étroites et cloud-native et une compatibilité élargie au cloud** pour vous aider à accélérer l'installation et la configuration initiales.
- **Performance.** Une solution SD-WAN capable d'identifier les **applications** (application-aware) est une solution aux problématiques de bande passante et de performances. La solution doit pouvoir identifier un large panel d'applications connues et utiliser des signatures personnalisées qui lui permettent de hiérarchiser le trafic et de gérer automatiquement les connexions en fonction des besoins en temps réel de l'entreprise.
- **Visibilité et contrôle.** L'identification des vulnérabilités au sein de différents environnements cloud relève de la gageure. Un SD-WAN géré en mode centralisé et capable de prendre en compte certains attributs du fournisseur de sécurité cloud (tagging par exemple) est à même de fournir une visibilité de bout en bout, nécessaire à des fonctions de prévention et de détection, et à une application automatisée des règles sur l'ensemble des clouds. Cette approche contribue également au respect des réglementations sectorielles et de la législation en matière de protection des données, quel que soit le lieu où les données sensibles sont stockées.

# Un SD-WAN efficace répond aux défis du multi-cloud

Une solution SD-WAN efficace peut concrétiser une infrastructure réseau de type « context-aware » couvrant plusieurs environnements cloud. Elle propose une infrastructure uniforme et cohérente, adossée à des règles, tout en simplifiant les tâches de gestion et en réduisant les coûts d'infrastructure. Elle renforce également l'agilité au sein des environnements et l'expérience applicative sur l'ensemble de l'entreprise. Enfin, des fonctions de sécurité intégrées offertes par une solution SD-WAN robuste et consolidée favorise la maîtrise des risques et le contrôle sur les infrastructures d'entreprise constituées de différents environnements Cloud.

Voici quelques questions à se poser pour sélectionner une solution SD-WAN adaptée au multi-cloud et sécurisée :

- Les fonctionnalités de sécurité et réseau sont-elles consolidées ?
- La solution offre-t-elle une visibilité de bout en bout et un contrôle granulaire de tous les environnements cloud ?
- Disposez-vous d'une console d'administration centralisée (interface unique) et de la possibilité d'appliquer des règles de manière globale ?
- Existe-t-il des tests pour valider les performances, la fiabilité ou la valeur (coût total de possession) de la solution dans les environnements cloud ?
- La solution prend-elle en charge les multiples et différents environnements de cloud privé et public ?

<sup>1</sup> Kim Weins, « [Cloud Computing Trends: 2020 State of the Cloud Report](#) », Flexera, 21 mai 2020.

<sup>2</sup> « [Global Infrastructure as a Service \(IaaS\) Market 2019-2023](#) », Business Wire, 23 octobre 2019.

<sup>3</sup> Charles McLellan, « [Multicloud: Everything you need to know about the biggest trend in cloud computing](#) », ZDNet, 01 juillet 2019.

<sup>4</sup> Sasha Emmerling, « [The Network Edge: Stretching the Boundaries of SD-WAN](#) », Network Computing, 07 août 2019.

<sup>5</sup> Ibid.

<sup>6</sup> Ibid.



[www.fortinet.fr](http://www.fortinet.fr)

Copyright © 2020 Fortinet, Inc. Tous droits réservés. Fortinet®, FortiGate®, FortiCare®, FortiGuard® et certaines autres marques sont des marques déposées de Fortinet, Inc., et les autres noms Fortinet mentionnés dans le présent document peuvent également être des marques déposées et/ou des marques de droit commun de Fortinet. Tous les autres noms de produit ou d'entreprise peuvent être des marques commerciales de leurs détenteurs respectifs. Les données de performances et autres indicateurs de mesure figurant dans le présent document ont été obtenus au cours de tests de laboratoire internes réalisés dans des conditions idéales, et les performances et autres résultats réels peuvent donc varier. Les variables de réseau, les différents environnements réseau et d'autres conditions peuvent affecter les performances. Aucun énoncé du présent document ne constitue un quelconque engagement contraignant de la part de Fortinet, et Fortinet exclut toute garantie, expresse ou implicite, sauf dans la mesure où Fortinet conclut avec un acheteur un contrat écrit exécutoire, signé par le directeur des affaires juridiques de Fortinet, qui garantit explicitement que les performances du produit identifié seront conformes à des niveaux de performances donnés expressément énoncés et, dans un tel cas, seuls les niveaux de performances spécifiques expressément énoncés dans ledit contrat écrit exécutoire ont un caractère obligatoire pour Fortinet. Dans un souci de clarté, une telle garantie sera limitée aux performances obtenues dans les mêmes conditions idéales que celles des tests de laboratoire internes de Fortinet. Fortinet rejette intégralement toute convention, déclaration ou garantie en vertu des présentes, qu'elle soit expresse ou implicite. Fortinet se réserve le droit de changer, de modifier, de transférer ou de réviser par ailleurs la présente publication sans préavis, et c'est la version la plus à jour de la publication qui est applicable. Fortinet rejette intégralement toute convention, déclaration ou garantie en vertu des présentes, qu'elle soit expresse ou implicite. Fortinet se réserve le droit de changer, de modifier, de transférer ou de réviser par ailleurs la présente publication sans préavis, et c'est la version la plus à jour de la publication qui est applicable.