

FICHE 4

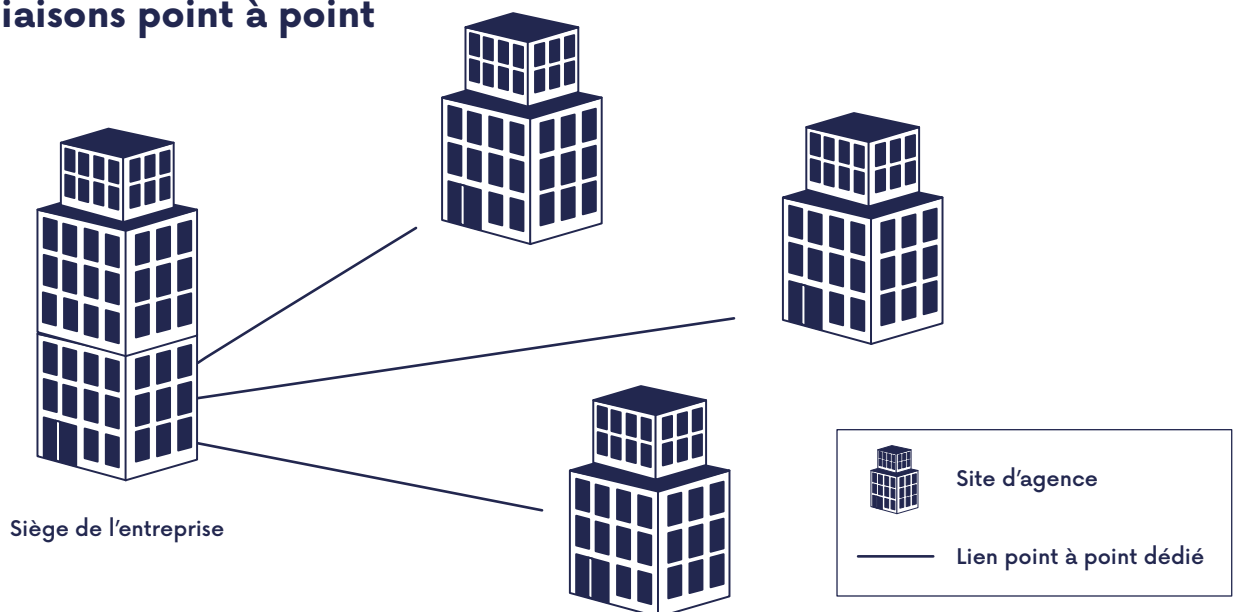
LES OFFRES DE RÉSEAUX INTERSITES

Les besoins télécoms des entreprises multisites imposent de connecter en un réseau sécurisé les différents sites d'une même entreprise. Ces réseaux permettent à la fois des échanges entre les sites de l'entreprise et l'accès à des ressources centralisées (données de l'entreprise et accès à des applications). On parle parfois de réseau étendu ou WAN (*Wide Area Network*), par opposition au réseau local¹ ou LAN (*Local Area Network*).

1 Il est possible d'utiliser des liaisons « point à point » entre les différents sites d'une même entreprise. Ce sont des réseaux privés physiquement isolés qui garantissent une sécurité et une disponibilité maximales. Les liaisons point à point reposent principalement sur les technologies fibre optique (fibre

noire ou fibre DWDM) ou sur les faisceaux hertziens, ou liaisons laser lorsque les deux sites sont en visibilité directe. Le coût d'une telle solution augmente fortement en fonction de la distance séparant les sites à relier entre eux.

Les liaisons point à point



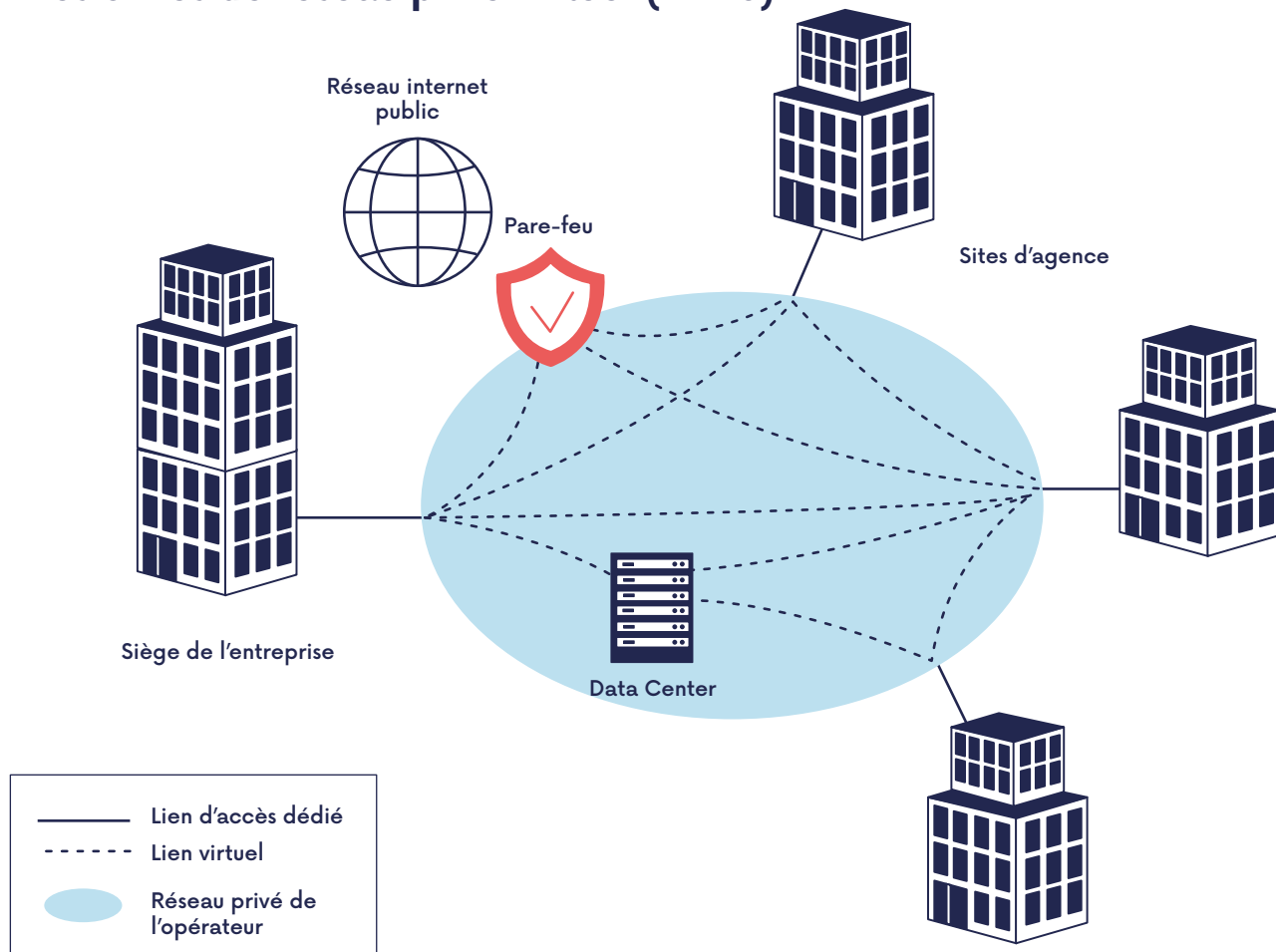
1. Les termes surlignés sont définis dans le glossaire en page 122.

2 Il est également possible de souscrire à une offre de réseau privé virtuel utilisant les réseaux MPLS (Multiprotocol Label Switching) des opérateurs pour sécuriser les flux intersites. Ce type de réseaux permet une isolation logique et sécurisée des flux entre les sites d'une même entreprise. La technologie VPN MPLS est aujourd'hui le **standard du marché** pour les réseaux avec un grand nombre de sites. Les liens d'accès du réseau interne de l'entreprise entre ses différents sites reposent sur toutes les technologies d'accès fixe (cuivre ADSL, cuivre SDSL, fibre optique dédiée, fibre optique FttH, 4G, etc.). Ces dernières sont détaillées dans la [FICHE 3 : Les offres d'accès fixe à internet](#).

L'intérêt de cette solution réside dans le fait que l'opérateur du réseau MPLS peut exercer une responsabilité sur les liens d'accès et le service réseau, garantir la sécurité et le chiffrement des échanges et mettre en place des mécanismes de priorisation des flux nécessitant un faible temps de latence, comme par exemple la voix sur IP.

Les fournisseurs de services de réseaux MPLS proposent également en option la possibilité d'accéder à des ressources centralisées, ainsi accessibles à l'ensemble des sites raccordés au réseau MPLS : par exemple, accès à des données ou applications situées dans un data center, accès à internet de manière sécurisée et centralisée.

Les offres de réseau privé virtuel (MPLS)

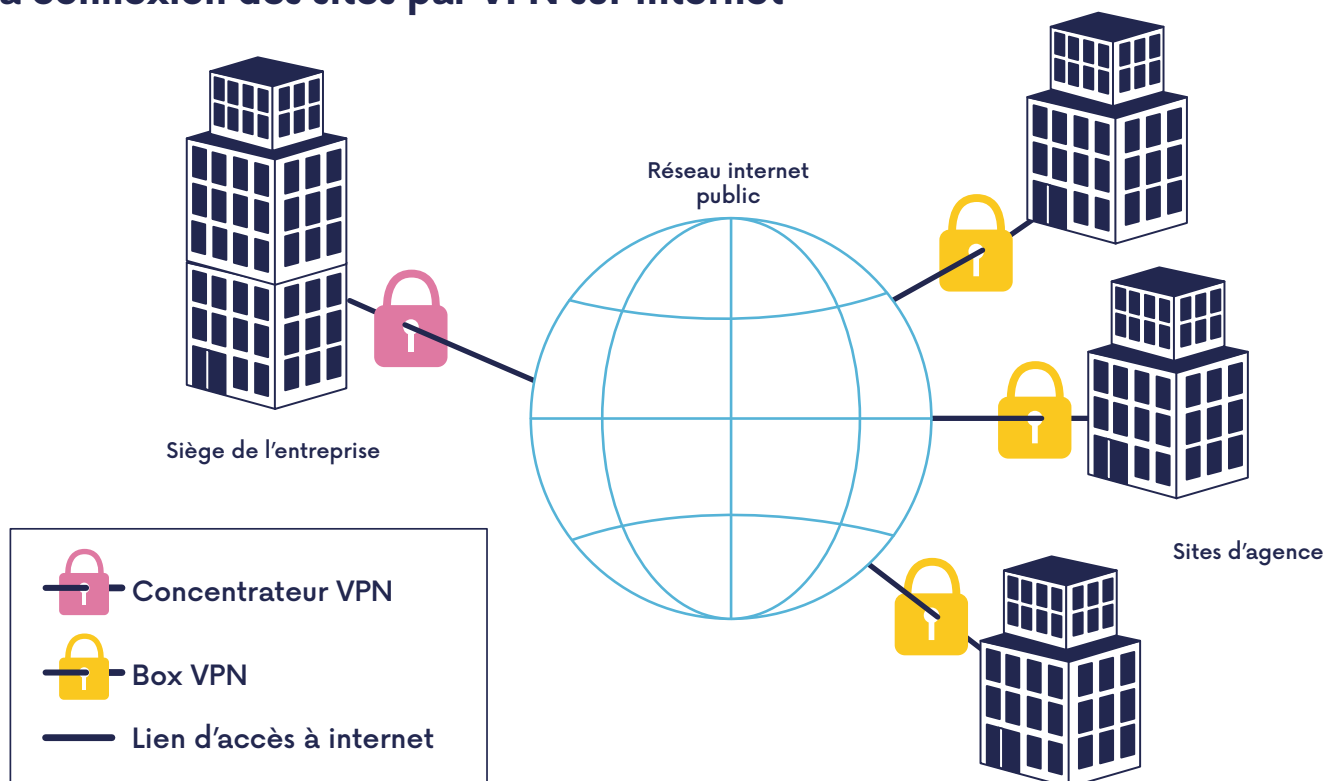


3 Les entreprises peuvent également disposer d'un accès internet pour chaque site et mettre en place une solution pour sécuriser les flux transitant par internet entre les sites distants, ou pour se connecter avec une entreprise partenaire (par exemple un client ou un sous-traitant). Les données transitant sur internet sont alors chiffrées et ne sont lisibles que par les utilisateurs vérifiés. On parle alors de **VPN sur internet**. Le protocole le plus fréquemment utilisé est IPsec.

Cette solution permet de la flexibilité dans le choix du fournisseur d'accès internet pour chaque site et une rapidité de mise en œuvre en réutilisant des accès internet préexistants.

La solution VPN sur internet peut aussi être complémentaire d'un réseau VPN MPLS, notamment pour la connexion des sites à l'international ou des sites éphémères (ex. événementiel) raccordés par exemple par une box 4G. Le concentrateur VPN sur internet peut également être situé sur le réseau de l'opérateur du réseau MPLS.

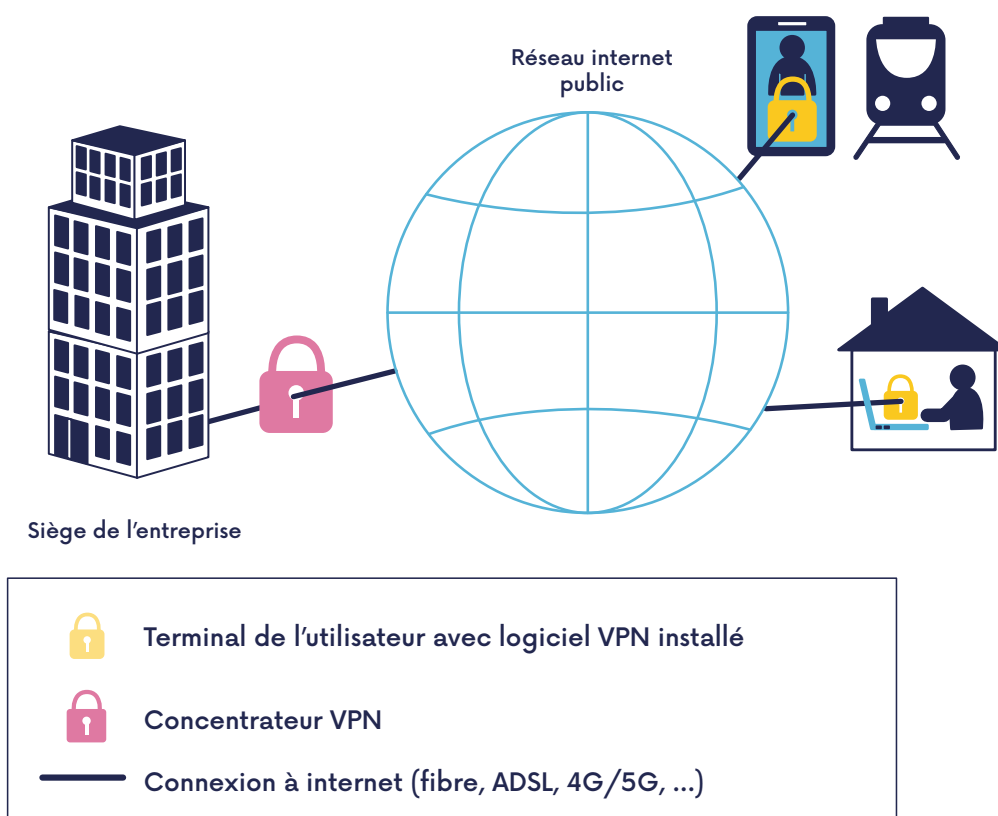
La connexion des sites par VPN sur internet



4 Les collaborateurs en télétravail ou déplacement ont besoin de se connecter à distance aux données de l'entreprise et aux logiciels métiers situés sur le site de l'entreprise ou dans un *cloud* privé. La sécurisation et le chiffrement de la connexion reposent sur un protocole de sécurisation des flux (les plus fréquents étant

IPsec ou SSL) entre le PC de l'utilisateur final équipé d'un logiciel VPN et un équipement de concentration VPN situé sur le site de l'entreprise. L'équipement de concentration VPN peut également être situé dans un data center (*cloud* privé de l'entreprise) ou sur le réseau de l'opérateur fournisseur du service MPLS.

La connexion externe des utilisateurs finals via un VPN sur internet



Certaines entreprises, disposant de plusieurs de sites, peuvent en complément utiliser l'architecture SD-WAN (*Software Defined WAN*). Cette architecture permet de centraliser la gestion de tous leurs équipements et accès réseau, même lorsqu'ils sont fournis par des opérateurs différents. Par exemple, il est possible d'appliquer, depuis une interface centralisée, une règle de sécurité à l'intégralité des accès réseau de l'entreprise, ou encore de choisir dynamiquement comment sont dirigées les requêtes des applications de tous les utilisateurs du réseau de l'entreprise, entre un accès internet local à chaque site et un accès internet centralisé de l'entreprise.

La mise en œuvre d'une architecture SD-WAN facilite le recours à des fournisseurs et à des technologies d'accès variés. La présence de plusieurs acteurs (fournisseur SD-WAN, intégrateur des équipements SD-WAN et opérateurs télécom) nécessite cependant de bien définir le domaine de responsabilité de chaque acteur afin d'assurer un diagnostic et une réparation rapide en cas d'incident.