Présentation du modèle Zero Trust Edge pour les services réseau et de sécurité

Une stratégie Secure Access Services Edge (SASE) se fonde sur un modèle Zero Trust Edge (ZTE)

par David Holmes et Andre Kindness
28 janvier 2021

Pourquoi lire ce rapport

Pour prendre en charge la transition numérique d'une entreprise en utilisant le cloud et l'Internet des objets (IoT), de nombreuses équipes réseau se sont tournées vers le SD-WAN. Cependant, le SD-WAN ne répond pas aux nouvelles exigences de sécurité ou à la fusion imposée entre le monde de la sécurité et celui de la mise en réseau. Nous recommandons aux professionnels I&O et S&R de lire ce rapport afin de mieux comprendre une solution Zero Trust émergente qui permettra d'unifier à la fois l'infrastructure réseau et l'infrastructure de sécurité pour prendre en charge la structure réseau à l'échelle de l'entreprise.

Points clés à retenir

Les cas d'utilisation en matière de sécurité guident les entreprises vers le ZTE

Le cas d'utilisation initial pour la plupart des entreprises en passe d'accéder au Zero Trust Edge (ZTE) consistera à garantir la sécurité et l'autonomie des télétravailleurs, tout en éliminant les VPN utilisateurs encombrants qui gangrènent actuellement le secteur.

Le chemin est encore long jusqu'à la clé de la réussite : la pile de sécurité hébergée à la périphérie de l'Internet

Le modèle ZTE tend à devenir une pile de sécurité complète hébergée dans le cloud ou en périphérie, mais la technologie n'est pas encore prête, car il existe d'autres dépendances. Tant que la bande passante reste limitée dans de nombreuses régions du monde, certains éléments devront être localisés.

La périphérie intelligente sur site : un moteur d'efficacité non négligeable

Les cas d'utilisation visant à prendre des décisions intelligentes sur site à la périphérie s'appliquent toujours, en particulier pour l'IoT/OT, la santé et les environnements de mise en réseau intense.

Présentation du modèle Zero Trust Edge pour les services réseau et de sécurité

Une stratégie Secure Access Services Edge (SASE) se fonde sur un modèle Zero Trust Edge (ZTE)

par David Holmes et Andre Kindness
avec Glenn O'Donnell, Joseph Blankenship, Paul McKay, Renee Taylor et Peggy Dostie

28 janvier 2021

Sommaire

2 **Fusionnez la sécurité et la mise en réseau, et sauvez votre entreprise du déclin**

Les approches historiques de la sécurité et de la mise en réseau ne sont pas compatibles avec l'entreprise distribuée

5 **L'émergence du Zero Trust Edge**

Surprise ! Le ZTE trouve sa source dans le cloud

Utilisez le ZTE pour déployer 18 services de sécurité et de mise en réseau

10 **Des cas d'utilisation pour dicter les types et les emplacements des services ZTE**

15 **Le marché propose différents types de choix ZTE**

De la place pour les piles multifournisseurs comme pour les piles à fournisseur unique

La complexité détermine également la nécessité d'utiliser une superposition via agent ou une passerelle sans agent

17 **Le Zero Trust Edge : une route semée d'embûches**

Implications

17 **La sécurité et la mise en réseau s'allient enfin contre un ennemi commun**

18 **Autres ressources**

Documents de recherche connexes

Evaluate SDWAN Services Based On Branch Office Goals, Not Hardware Data Sheets (Evaluer les services SDWAN en fonction des objectifs des succursales, et non des fiches techniques matérielles)

Now Tech: Software-defined WAN Hardware/ Software, Q3 2020 (Now Tech : Matériel/logiciel WAN défini par logiciel, T3 2020)

Now Tech: Software-defined Service WAN, Q3 2020 (Now Tech : Services WAN définis par logiciel, T3 2020)

FORRESTER®

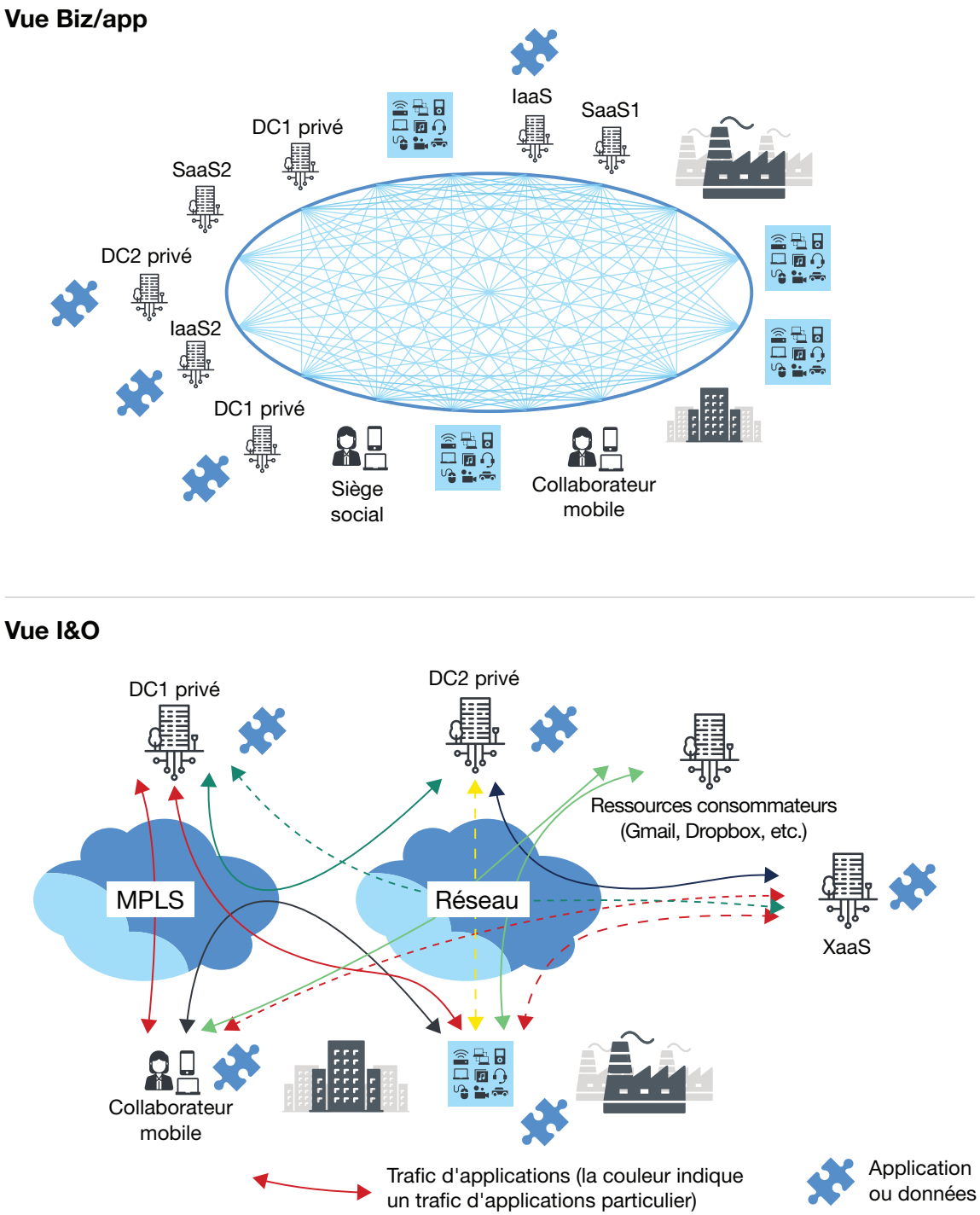
Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 Etats-Unis
+1 617-613-6000 | Fax : +1 617-613-5000 | forrester.com

Fusionnez la sécurité et la mise en réseau, et sauvez votre entreprise du déclin

La sécurité et la mise en réseau partagent depuis longtemps une histoire complexe, que l'on pourrait décrire comme cordiale, au mieux, ou hostile, au pire. Cependant, cette approche dichotomique n'est pas acceptable et sabote souvent les avantages obtenus grâce aux initiatives numériques. Les infrastructures et opérations de sécurité et de mise en réseau cloisonnées disparaissent rapidement pour les raisons suivantes :

- **Les données et les applications distribuées dans le cloud sont accessibles en dehors du datacenter.** Non seulement le cloud, la périphérie et l'IoT redéfinissent l'emplacement des données et des applications, mais ces composants de numérisation ont également mis fin à la conception de réseau traditionnelle en étoile[1]. Désormais, une structure de mise en réseau à l'échelle de l'entreprise interconnecte les actifs métier, les clients, les partenaires et les ressources numériques afin de relier tous les éléments de l'écosystème métier (voir Figure 1)[2]. Comme le signale le rapport de Forrester intitulé « Build Security Into Your Network's DNA: The Zero Trust Network Architecture » (Intégrer la sécurité à l'ADN de votre réseau : l'architecture réseau Zero Trust), cela ne peut se produire que si la sécurité est intégrée à l'ADN du réseau.
- **La COVID-19 a poussé les collaborateurs hors du contrôle d'une infrastructure LAN d'entreprise.** Considérez cette réalité toute simple : aujourd'hui, de nombreuses applications professionnelles existent dans le cloud, et ce chiffre ne fait qu'augmenter. Les utilisateurs ont eux aussi quitté l'enceinte traditionnelle de l'entreprise ; l'enquête menée par Forrester sur l'expérience pandémique a révélé que 53 % des nouveaux télétravailleurs veulent continuer de travailler à distance, même après la crise[3]. Les applications et les utilisateurs ne se trouvant plus dans cette enceinte, l'utilité et la valeur de la pile de sécurité qui en dépend se sont effondrées.

FIGURE 1 La dispersion des applications et des données à travers les ressources de l'entreprise



Les approches historiques de la sécurité et de la mise en réseau ne sont pas compatibles avec l'entreprise distribuée

A cause de la pandémie de 2020, des millions de collaborateurs ont dû quitter le cocon de l'entreprise pour entrer soudainement dans le télétravail, cette grande inconnue. Le CISO d'une grande compagnie d'assurance européenne nous a confié qu'avant la pandémie de 2020, l'entreprise pratiquait 5 % de télétravail. La pandémie a inversé le ratio, et les travailleurs à domicile représentent maintenant 95 % de la base de collaborateurs. Pour des entreprises de ce type, l'infrastructure VPN déjà bancale ne faisait pas le poids. La technologie VPN n'est qu'une autre faille dans l'enceinte traditionnelle érodée. Les équipes chargées de la sécurité et de la mise en réseau ont rencontré des difficultés à répondre aux nouvelles exigences en matière d'utilisation du cloud et de prise en charge des télétravailleurs, car les anciennes approches se fondaient sur les points suivants :

- **Des appliances matérielles ou logicielles dédiées sur site.** L'époque où l'on introduisait un type de solution spécifique pour résoudre un problème technologique particulier est révolue. Trente ans de connexion d'appareils au réseau, tels que les optimiseurs WAN ou les pares-feux, ont engendré plus de problèmes de sécurité, plus de complexité, moins de flexibilité et moins d'efficacité. Chaque nouvel appareil accroît de manière exponentielle la complexité et les problèmes de sécurité potentiels.
- **Des contrôles sur site et des référentiels de politiques peu fiables.** Les logiciels de gestion sur site ont besoin de matériel et de personnel dédiés pour rester à jour et s'équiper des dernières fonctionnalités, des nouveaux correctifs et des améliorations de sécurité. Les logiciels de gestion qui résident dans une infrastructure privée coûtent non seulement plus cher à l'entreprise, mais ils entravent également les capacités de résilience. Les logiciels ne sont généralement pas conçus pour être déplacés vers des plates-formes cloud, ce qui limite l'efficacité et les options de reprise après sinistre.
- **La limitation de l'approche centrée sur le matériel.** Les avions, les voitures et les trains sont soumis à des restrictions en matière de forme et de conformité en raison de contraintes de poids ou de taille. Même sans ces contraintes, les équipes technologiques ne sont pas en mesure d'introduire du matériel dans chaque partie du site de fabrication, du magasin ou du stade. Il est impossible d'imaginer du matériel créé pour répondre aux exigences de forme, de fonction et de conformité entre la machine d'extrusion de plastique et l'étuve chauffée ou pour survivre aux températures dans lesquelles l'équipement doit fonctionner dans des endroits tels qu'une sous-station électrique de Dubaï ou une station cellulaire de la vallée de la Mort.
- **Des silos de sécurité et de mise en réseau disjoints.** La pratique consistant à reléguer certains types de matériel et d'opérations à certains groupes ne fait qu'augmenter les inefficacités opérationnelles, réduire la résilience de l'infrastructure et potentiellement créer des problèmes de sécurité. De nombreux dispositifs discrets, tels que les pares-feux et les routeurs, peuvent être combinés pour réduire la latence en utilisant une table unique pour rechercher des règles concernant les paquets et appliquer des politiques de sécurité et de mise en réseau au niveau du port.

L'émergence du Zero Trust Edge

Lorsque la pandémie de COVID-19 a forcé les collaborateurs à travailler à domicile, une minorité de professionnels de la sécurité avant-gardistes, convaincus que la technologie VPN ne constituait pas la meilleure voie, a investi dans des solutions d'accès réseau Zero Trust (ZTNA) pour contourner les problèmes liés aux VPN. Certains d'entre eux ont demandé s'il existait d'autres approches ZT à adopter, étant donné que de nombreux professionnels de la sécurité et de l'I&O considéraient principalement le Zero Trust comme un concept de datacenter (voir Figure 2) [4]. Cependant, le cadre de sécurité défini dans le rapport de Forrester intitulé « The Zero Trust eXtended (ZTX) Ecosystem » (L'écosystème Zero Trust eXtended (ZTX)) montre pourquoi le ZT est bien plus qu'un concept de datacenter. Le ZT protège les entreprises des clients, des collaborateurs, des sous-traitants et des appareils des sites distants qui se connectent via des réseaux WAN à un environnement plus hostile, ouvert, dangereux et turbulent (voir Figure 3). Forrester considère ce concept comme un modèle Zero Trust Edge (ZTE) et le définit comme suit :

> *Une solution Zero Trust Edge connecte et transporte en toute sécurité le trafic, en utilisant les principes d'accès Zero Trust, dans et en dehors des sites distants qui exploitent principalement des services de sécurité et de mise en réseau basés sur le cloud.*

FIGURE 2 Les premiers utilisateurs du ZT considéraient que les micropérimètres de sécurité ne concernaient que les VM

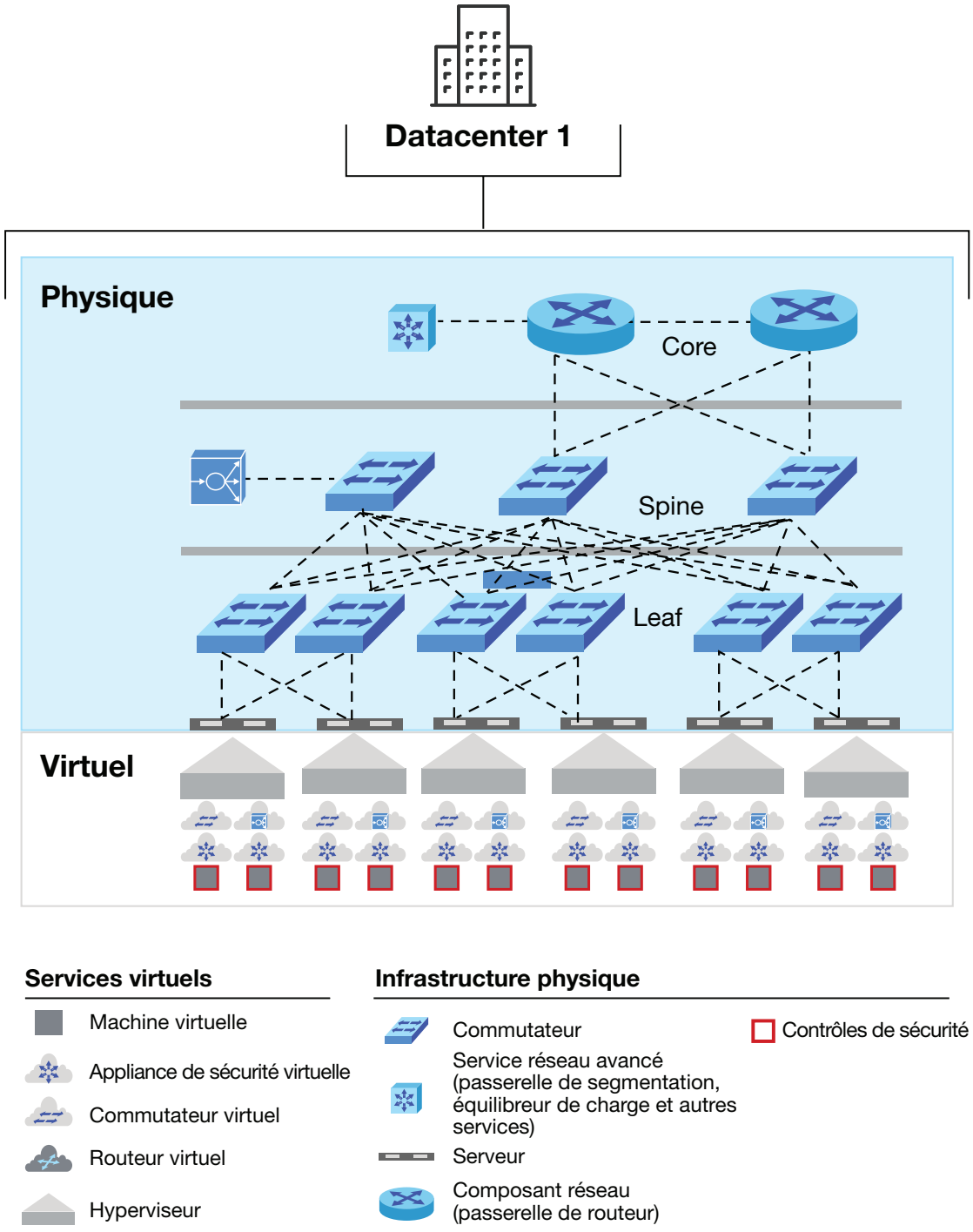
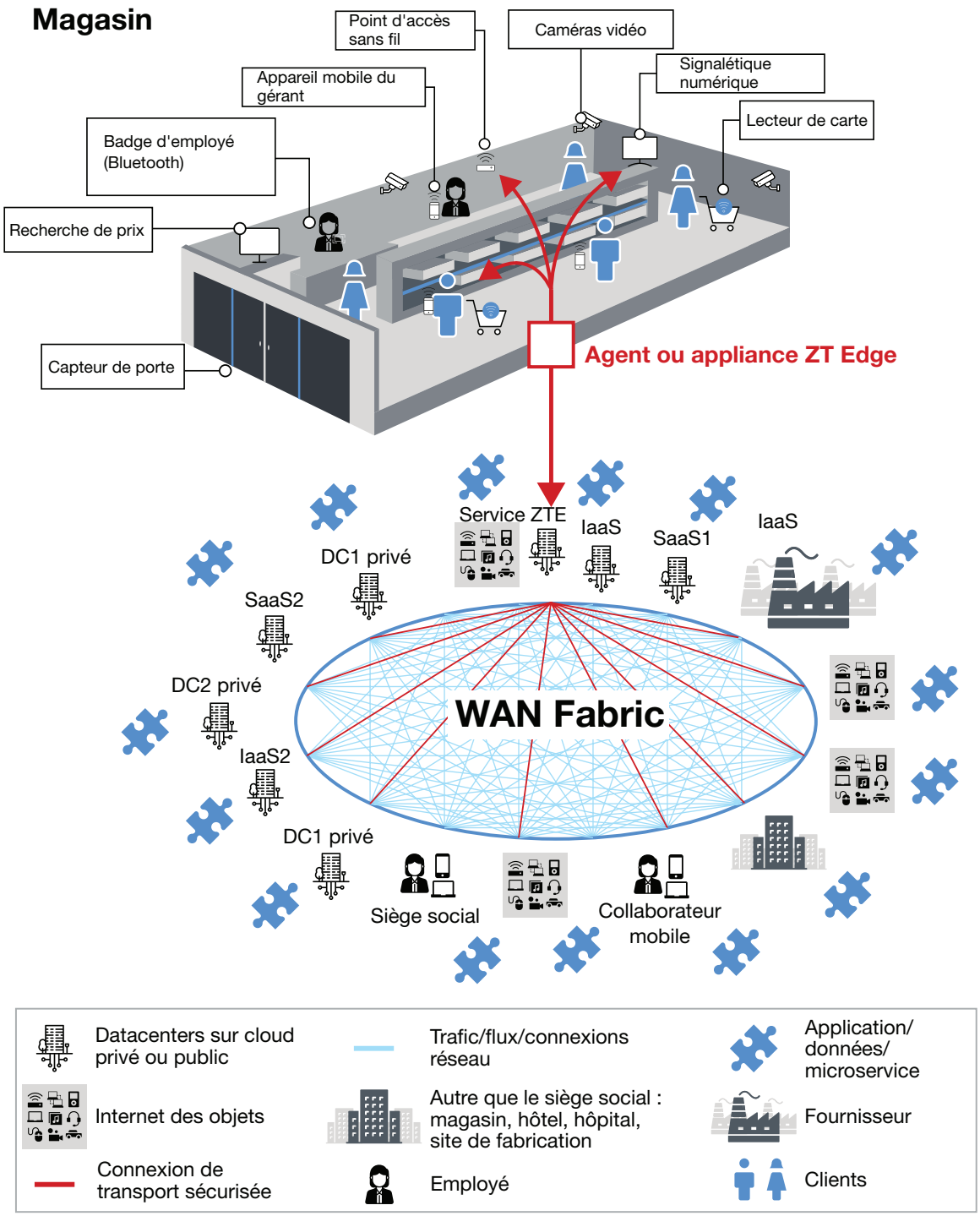


FIGURE 3 Le ZTE fournit les contrôles de sécurité et les politiques de mise en réseau pour sécuriser toutes les connexions sur site



Surprise ! Le ZTE trouve sa source dans le cloud

Le ZTE définit la structure de sécurité et de mise en réseau autour du trafic et des services provenant de sites distants dans les entreprises, ainsi que les services renvoyés aux sites ou utilisateurs. Tandis que le ZTE s'occupe de l'entreprise distribuée, les solutions, qui offrent un ensemble de services plus rapides et plus agiles, doivent être conçues sur deux éléments essentiels :

- **La gestion du réseau et de la sécurité dans le cloud.** Historiquement, les configurations des appareils et les politiques de sécurité ont toujours existé dans différents outils. Par exemple, les contrôles d'accès réseau comporteraient des politiques de sécurité pour les utilisateurs, tandis que les solutions de gestion pour les pares-feux et les composants réseau contenaient les configurations des appareils. Cette situation augmente le nombre d'erreurs de configuration et réduit les rendements opérationnels à mesure que le personnel définit des politiques similaires sur plusieurs systèmes. La gestion du cloud permet de fusionner ces systèmes back-end disparates et de modifier, d'ajouter ou de supprimer des configurations en se basant sur une seule solution de gestion.
- **Surveillance et analyse basées sur le cloud.** La mise en réseau et la surveillance de la sécurité sont généralement indépendantes l'une de l'autre et constituent des exigences fondamentales de l'existence du ZTE. Google en est l'illustration parfaite : la société utilise son réseau WAN défini par logiciel pour atteindre 100 % d'utilisation sur les liens. La surveillance identifie les irrégularités du trafic (souvent des problèmes de sécurité) jusqu'aux peering metros et loin des datacenters de l'entreprise[5]. La quantité d'informations à recueillir et à synthétiser oblige à baser la surveillance ZTE sur le cloud. Pour bénéficier d'une analyse complète, il est nécessaire d'utiliser une plate-forme informatique aussi étendue.

Utilisez le ZTE pour déployer 18 services de sécurité et de mise en réseau

Partout dans le monde, les entreprises peuvent gérer, surveiller et analyser de manière centralisée l'ensemble des services de sécurité et de mise en réseau qui résident dans les solutions ZTE (voir Figure 4). Certains de ces services resteront exclusivement dans le cloud (ou le cloud edge), tandis que d'autres devront être hébergés à distance.

FIGURE 4 Type de services disponibles dans une solution ZTE

Réseau

Garantie de bande passante	Définit une quantité minimale de bande passante pour un trafic particulier
Mise en cache du contenu	Fournit des copies localisées des données
Equilibrage et utilisation des liens	Exploite plusieurs liens simultanément pour augmenter la bande passante du trafic et l'utilisation du WAN dans son ensemble
Qualité du service	Donne la priorité au trafic réseau
Résilience	Fournit et maintient un niveau de service acceptable en cas de défaillances et de difficultés liées au fonctionnement normal
Routage/meilleur chemin	Sélectionne le chemin approprié pour le transport de couche 3, même entre le télétravailleur et l'application hébergée dans le cloud
WAN défini par logiciel (SD-WAN)	Choisit les meilleurs chemins, liens ou connexions en fonction de mesures de niveau supérieur, telles que l'instabilité, les paquets perdus et l'affinité avec un profil d'application
Connexion WAN	Etablit la connexion physique vers/depuis un site
Optimisation WAN	Offre des fonctionnalités de déduplication, d'union des paquets et d'optimisation WAN

FIGURE 4 Type de services disponibles dans une solution ZTE (suite)

Sécurité

Pare-feu de base	Offre des fonctionnalités de pare-feu réseau simples (règles de couche 3 et 4) qui peuvent être séparées et déplacées localement pour réduire la quantité de trafic sortant du site distant
Agent de sécurité d'accès au cloud (CASB)	Contrôles et rapports sur l'accès aux applications cloud
Pare-feu as a service (FWaaS)	Fournit des fonctionnalités de pare-feu avancées basées sur le cloud
Système de détection/prévention des intrusions (IDS/IPS)	Analyse le trafic réseau en fonction des signatures afin de détecter et de détourner du contenu malveillant spécifique
Chiffrement des liens	Chiffre et déchiffre tout le trafic réseau à chaque point de routage réseau
Gestion des identités et des accès (IAM)	Vérifie que les personnes habilitées d'une entreprise disposent de l'accès approprié aux ressources technologiques
Passerelle Web sécurisée (SWG)	Empêche le trafic non sécurisé d'entrer dans le réseau interne d'une organisation. Les filtres d'URL doivent être constamment mis à jour et, comme c'était déjà la tendance, configurés, hébergés et gérés dans le cloud
Analyse avancée des logiciels malveillants	Exécute des programmes dans un environnement isolé (sandboxing) pour surveiller et contenir les logiciels malveillants de type zero-day
Accès réseau Zero Trust (ZTNA)	Permet au télétravailleur de se connecter aux applications d'entreprise en fonction de son identité, quel que soit l'emplacement des employés ou des applications. Il s'agit du service de sécurité relatif aux signatures, qui doit exister dans le ZTE.

Des cas d'utilisation pour dicter les types et les emplacements des services ZTE

Les architectes réseau et de sécurité doivent garantir un maximum d'utilité à mesure qu'ils tendent vers le Zero Trust Edge. Les types de services utilisés dépendent de l'emplacement, des appareils, des personnes et d'autres éléments (voir Figure 5). Trois cas d'utilisation montrent des niveaux croissants d'éléments contraignants (ce qui signifie une augmentation du nombre de services de sécurité et de mise en réseau activés dans la solution ZTE) :

- **La sécurisation des télétravailleurs dans le cadre du cas d'utilisation initial.** La pandémie de 2020 et l'exode massif qui en a résulté a renvoyé des millions de cadres à la maison. La distribution d'un accès sécurisé aux services et applications de l'entreprise pour ces travailleurs

à domicile constitue le cas d'utilisation initial grâce auquel les entreprises ont pu accéder au Zero Trust Edge. En raison des nombreux défis décrits dans l'étude de Forrester, « Key Considerations For Network And Capacity Management When Operationalizing A Home-Based Workforce » (Principales préoccupations concernant la gestion réseau et des capacités pour rendre opérationnel l'effectif à domicile), la plupart des entreprises ont renoncé à installer des logiciels ou du matériel réseau à l'intérieur de la maison. Elles ont préféré déployer des agents logiciels sur les appareils professionnels des travailleurs et relier leurs connexions aux services de sécurité du cloud edge (voir Figure 6).

- **Hiérarchisation du trafic des applications professionnelles qui domine le réseau WAN de la succursale.** Le nombre de connexions WAN a explosé en raison du télétravail. Néanmoins, les connexions distantes ont constitué la majeure partie du trafic WAN d'une entreprise, principalement en provenance des collaborateurs, de leurs applications et des appareils appartenant à l'entreprise. Le trafic SaaS, tel que O365, est récemment devenu un facteur majeur et peut également contenir une part de trafic client. Le trafic des applications SaaS nécessite des connexions directes à Internet, et les clients peuvent avoir besoin de se connecter à des réseaux LAN distants. Pour relever ces défis, les architectes d'entreprise dirigent de plus en plus ce trafic via le pare-feu as a service (FWaaS). Cette opération s'effectue par le biais de routeurs distants et/ou de solutions SD-WAN mises en avant dans le rapport de Forrester « Now Tech: Software-Defined WAN Hardware/Software, Q3 2020 » (Now Tech : Matériel/logiciel WAN défini par logiciel, T3 2020) ou auprès d'un fournisseur de services répertorié dans le rapport de Forrester « Now Tech: Software-Defined WAN Services, Q3 2020 » (Now Tech : Services WAN définis par logiciel, T3 2020) (voir Figure 7). Certains fournisseurs, comme Forcepoint, prennent en charge la fonctionnalité SD-WAN intégrée à plusieurs services de sécurité.
- **Enfin, la sécurisation de l'Internet de tous les objets.** Outre les télétravailleurs et les succursales génériques, l'IoT, les appareils de périphérie et les partenaires commerciaux utilisent fortement le réseau. L'architecte de supervision (Industrial Control System, ICS) devra intégrer les sites concernés dont les politiques réseau et de sécurité exigent une attention accrue. Par exemple, dans une usine automobile, un ingénieur tient compte du trafic provenant des collaborateurs et des sous-traitants, ainsi que du trafic provenant des automates programmables industriels (PLC, programmable logic controllers) de Siemens ou des données décrivant le poids des étagères de contrôle des stocks de Bosch. En raison de l'emplacement et du manque de bande passante sur le site, certains éléments de sécurité de base doivent être hébergés sur site, de même que tous les services réseau, afin de réduire la quantité de trafic dirigé vers les services de sécurité dans le cloud (voir Figure 8).

FIGURE 5 Chaque cas comporte un ensemble différent de facteurs de sécurité et de mise en réseau à prendre en compte

	Télétravail	Petit bureau	Site hétérogène
Actifs	Ordinateur portable	Ordinateurs de bureau, imprimantes, salles de conférence, webcams	Réseau physique hétérogène
Passerelle vers ZTE	Agent de points de terminaison	Appareil WAN avec services réseau sur site requis ou superposition via agent	Appareil WAN avec services réseau sur site requis
IoT	Non	Faible	Elevé
Informatique edge	Non	Faible	Elevé
Sous-traitants	Non	Non	Oui
Fournisseurs commerciaux et technologiques	Non	Faible	Elevé

FIGURE 6 Les télétravailleurs bénéficient des services de sécurité basés sur le cloud du ZTE

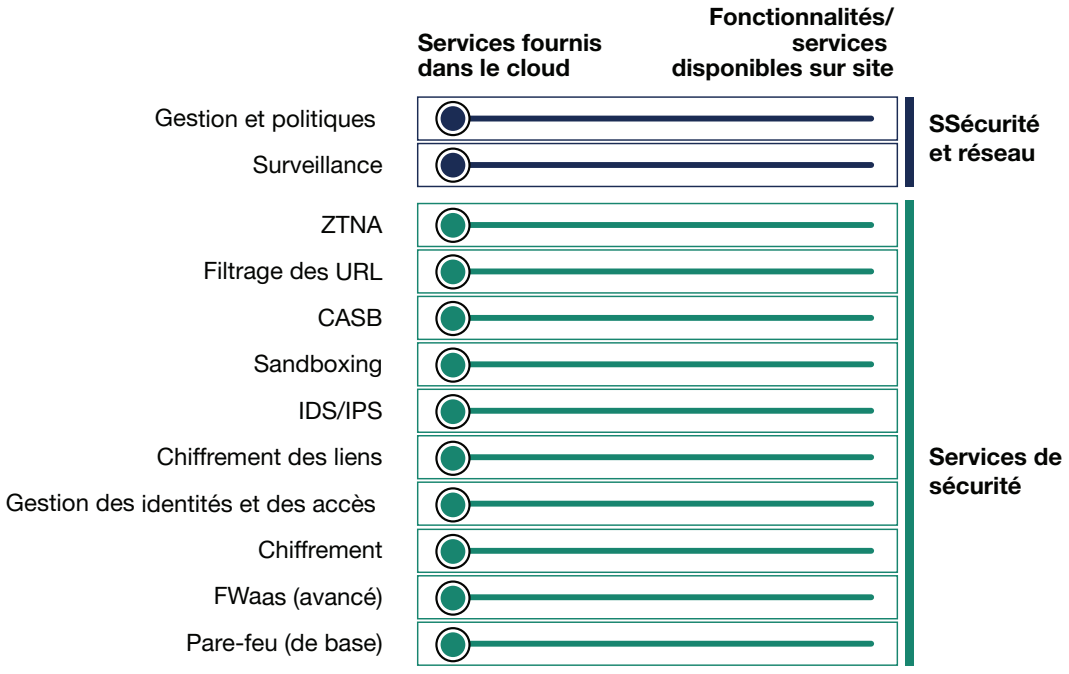


FIGURE 7 Les bureaux professionnels génériques assurent la direction du trafic vers les services de sécurité basés sur le cloud

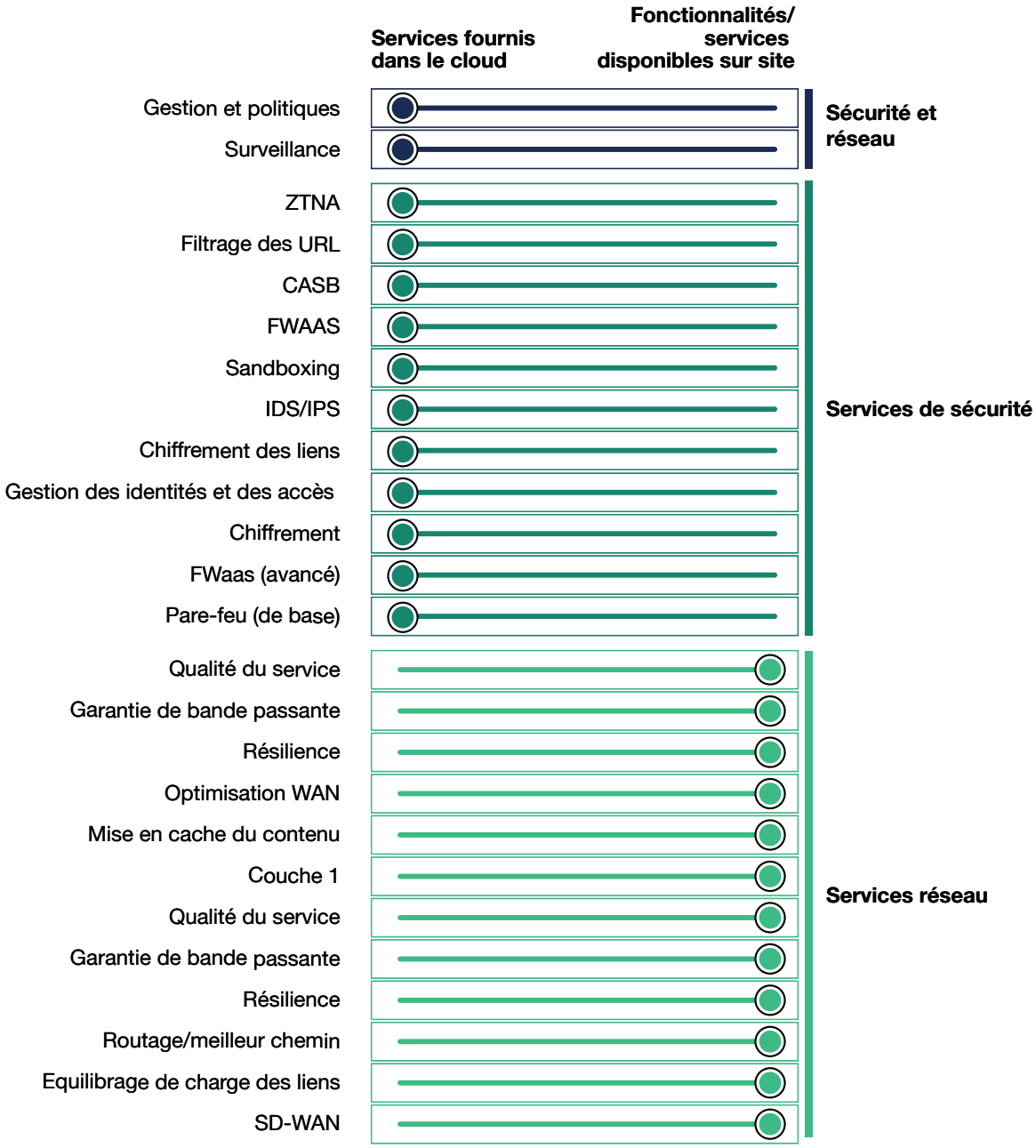
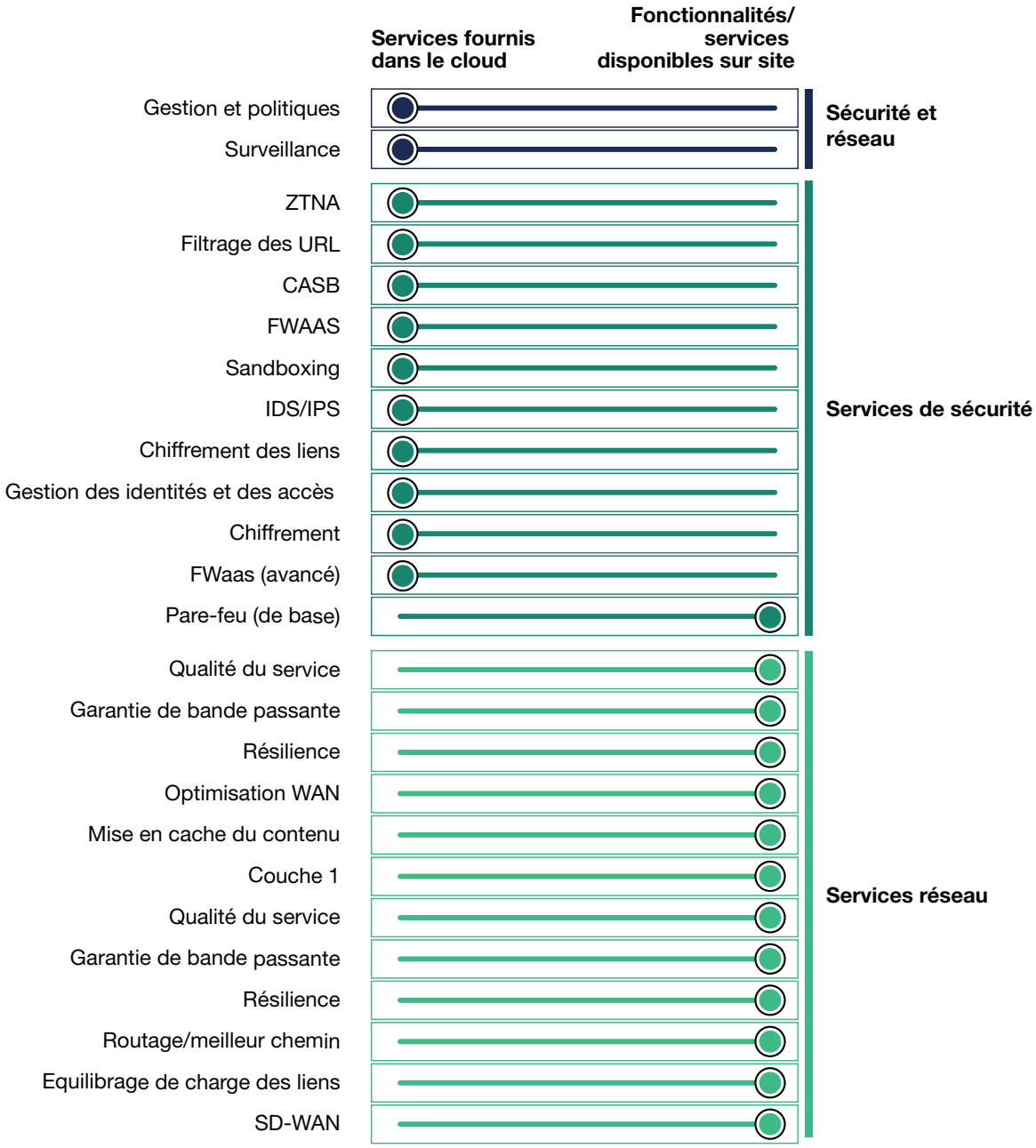


FIGURE 8 Des sites complexes avec bande passante WAN limitée exigent certaines fonctionnalités de sécurité localisées



Le marché propose différents types de choix ZTE

Les professionnels de la technologie peuvent tirer parti du ZTE en passant par trois méthodes différentes :

- **Un service fourni dans le cloud.** Issus de fournisseurs relativement nouveaux, les services basés sur le cloud du ZTE proviennent d'un service géré par un fournisseur comme Cato Networks, utilisant un réseau tiers avec des dizaines, voire des centaines, de points de vente proposant des fonctionnalités ZTE de cloud edge. Cette approche offre toute la valeur que les organisations peuvent tirer des solutions de logiciel SaaS. Cependant, aucune entreprise ne peut fournir toutes les fonctionnalités offertes par les meilleures solutions du marché. Bien sûr, Forrester a constaté que les organisations n'utilisent pas, en temps normal, toutes les fonctionnalités des solutions sur site. Les solutions cloud répondent souvent aux besoins de nombreuses entreprises.
- **Des services ZTE intégrés à un service de connexion WAN.** D'autres professionnels incluent un opérateur télécom d'entreprise existant en connectant ses clients directement aux réseaux ZTE pour fournir des fonctions de sécurité externalisées. Comcast Enterprise et Akamai remplissent déjà cette fonction aujourd'hui. De nombreux fournisseurs de matériel et de logiciels SD-WAN, tels que Versa Networks, créent des partenariats avec Zscaler ou d'autres fournisseurs de sécurité. Les équipes peuvent choisir les meilleurs produits du marché pour bénéficier de tous les avantages des services de sécurité et de mise en réseau. Cependant, elles ne profiteront pas de l'agilité ou du rendement opérationnels des systèmes basés sur le cloud. Pour adopter une approche intégrant le SD-WAN et le ZTE, les équipes technologiques doivent prendre des mesures supplémentaires, telles que la configuration de politiques pour chaque service indépendant. Il n'existe aucun système unique de gestion et d'orchestration pour une stratégie d'intégration du SD-WAN et du ZTE.
- **Une approche DIY (do it yourself).** Une organisation suffisamment grande et agile pourrait créer sa propre plate-forme ZTE en sollicitant des fournisseurs de services cloud pour faire office de points de vente et un service hébergé dans le cloud, comme le pare-feu d'entreprise de Barracuda, pour faire office de service de sécurité dans le cloud Azure de Microsoft. Ainsi, les professionnels s'assurent que les services répondent plus étroitement aux besoins de l'entreprise. Toutefois, cette démarche suppose que les équipes sont en mesure d'évaluer les besoins de l'entreprise et disposent des compétences nécessaires pour créer l'infrastructure et la gérer. Le rapport de Forrester intitulé « Evaluate SD-WAN Services Based On Branch Office Goals, Not Hardware Data Sheets » (Evaluer les services SD-WAN en fonction des objectifs des succursales, et non des fiches techniques matérielles) montre qu'il manque un ou plusieurs éléments à la plupart des équipes.

De la place pour les piles multifournisseurs comme pour les piles à fournisseur unique

Le ZTE représente une menace existentielle pour de nombreuses solutions de sécurité sur site. Une stratégie ZTE est donc désormais essentielle pour ces fournisseurs. Les fournisseurs ambitieux souhaitent vous vendre l'ensemble du package clé en main (lorsqu'ils en possèdent un), et l'idée de ne faire appel qu'à un seul fournisseur pour toutes les solutions de sécurité sur une base OPEX sera intéressante pour les PME et les marchés de taille intermédiaires. Votre choix dépend de la taille et de la complexité de votre organisation, pour les raisons suivantes :

- **Les grandes entreprises opteront pour une approche multifournisseur à court terme.** Elles ont des exigences plus complexes et des services plus hétérogènes. Une charge plus conséquente d'applications héritées les rend moins susceptibles d'adopter une approche à fournisseur unique. Les personnes interrogées dans le cadre de cette étude étaient toutes d'accord sur cette analyse. Pour les entreprises qui ont déjà commencé une transition vers le Zero Trust Edge, une approche multifournisseur classique peut utiliser les Silver Peak Systems pour le SD-WAN en se connectant à Zscaler pour le filtrage des URL et du ZTNA. Cette solution fonctionne pour le cas d'utilisation initial (sécurisation des télétravailleurs), mais la migration d'autres éléments de pile de sécurité vers une pile multifournisseur nécessite un chaînage de services méticuleux. De plus, les API entre les composants doivent fonctionner de manière cohérente et fiable.
- **Les petites entreprises sont les pionnières de l'approche de la pile de sécurité complète.** Forrester s'attend à ce qu'elles essaient des fournisseurs ZTE de piles complètes, tels que Netskope. En général, leurs exigences sont plus faibles, si bien qu'elles peuvent préférer solliciter un seul fournisseur, plus facile à aborder. Jusqu'ici, l'adoption de ces types de solutions a toujours nécessité l'intervention de plus grands groupes de technologies d'entreprise. Par exemple, cette situation s'est produite sur le marché du Wi-Fi avec les solutions basées sur le cloud d'Aerohive Networks, qui fait désormais partie d'Extreme Networks, et de Meraki, qui fait maintenant partie de Cisco.

La complexité détermine également la nécessité d'utiliser une superposition via agent ou une passerelle sans agent

La connexion de tous les utilisateurs et toutes les applications constitue l'état final visé par le Zero Trust Edge, que les systèmes soient sur site, dans le cloud, dans un cloud privé ou à distance. Cependant, la connexion d'un réseau complexe et hétérogène exige des efforts considérables. Par conséquent, le marché prend actuellement en charge deux types de déploiements, l'un visant l'état final stratégique et l'autre visant une entrée stratégique dans le Zero Trust Edge. Certains fournisseurs, comme Zscaler, peuvent prendre en charge les deux modèles simultanément, et de plus en plus de fournisseurs font de même.

- **Premier modèle : une passerelle est un point de sécurité unique.** Ce modèle devient votre point d'entrée unique vers Internet. Imaginez un contrôleur SD-WAN doté d'un tunnel GRE vers un réseau de périphérie hébergé par un fournisseur. Tout le trafic sortant se dirige ensuite vers le réseau de périphérie, qui peut ensuite attribuer immédiatement des politiques de sécurité au trafic de ce locataire sur son réseau. Le risque de menace provenant de la source d'origine diminue considérablement, ce qui élimine totalement les attaques de type DDoS. Bien que cette option soit la plus propre, elle est plus susceptible d'être adoptée dans le marché intermédiaire du fait de sa possible incompatibilité avec les environnements hétérogènes compliqués à court terme.
- **Second modèle : une superposition distribue la sécurité, généralement via des agents.** Dans ce modèle, les terminaux se connectent au réseau de périphérie via une superposition, généralement facilitée par un agent de points de terminaisons qui détermine quelles connexions sont redirigées vers le réseau ZTE. Le modèle de superposition peut être mis en œuvre sans modification du réseau sous-jacent. Toutefois, cette opération risque d'être compromise car l'installation d'agents peut s'avérer impossible en raison de la présence de politiques dans des environnements sensibles tels que les soins de santé, la fabrication et l'informatique/OT. Axis Security adopte une approche innovante qui utilise le modèle de superposition sans faire appel à des agents sur les appareils qui tentent de rejoindre le réseau. Nous avons interrogé un client important qui a choisi la solution Axis Security pour cette même raison.

Le Zero Trust Edge : une route semée d'embûches

Le modèle Zero Trust Edge est révolutionnaire, car il transforme la manière dont la sécurité et la mise en réseau sont traditionnellement utilisés. En constante évolution, les fonctions de cybersécurité sont passées plus rapidement au Zero Trust Edge. Les réseaux hérités seront beaucoup plus lents. Les entreprises se mettent au Zero Trust Edge en raison du problème de sécurité des télétravailleurs, mais des défis importants les attendent pour réaliser le plein potentiel du modèle, notamment les suivants :

- **Des applications et services existants.** Les applications Web modernes comprennent la fédération d'identité, ce qui les rend (relativement) faciles à configurer dans un ZTE. Cependant, les applications basées sur des protocoles non Web, en particulier les RDP/VDI et SIP/VoIP, ne seront pas si faciles à gérer. Même ces deux types d'applications très courants souffrent de l'absence d'une méthode standardisée de consommation dans l'environnement ZTE.
- **Un équipement de mise en réseau existant.** Après avoir intégré les ordinateurs portables, les serveurs et les applications au Zero Trust Edge, l'architecte doit prendre en compte les milliers, voire les centaines de milliers, d'appareils OT et IoT sur lesquels aucun logiciel d'agent ne peut être installé. Il doit procéder à une intégration en masse, en utilisant les protocoles de mise en réseau acceptés, ce qui implique une coopération entre les équipes de sécurité et celles de mise en réseau.
- **La capacité et la confiance.** Les entreprises peuvent utiliser le ZTE pour résoudre de manière stratégique des problèmes tels que l'accès sécurisé pour les télétravailleurs. Cependant, elles ne sont pas encore prêtes à remplacer les services de réseau et de sécurité haute capacité qui gèrent leurs datacenters existants. Les entreprises qui ont déjà investi massivement dans leurs propres datacenters attendront une initiative plus importante, comme la migration dans le cloud de leurs applications critiques, avant de transférer ces services vers la protection de type Zero Trust Edge.

Implications

La sécurité et la mise en réseau s'allient enfin contre un ennemi commun

La sécurité étant incorporée au réseau et faisant partie intégrante de son ADN, Forrester prévoit les scénarios suivants pour les deux organisations :

1. **Organisations de sécurité définissant les politiques et les tests de sécurité.** Les types de trafic et les services nécessaires pour atteindre des niveaux de confiance acceptables seront définis par l'équipe de sécurité. Grâce à des outils de surveillance et d'analyse, les équipes s'assureront du respect des politiques. Elles testeront et auditeront régulièrement le trafic et les connexions, ensemble.
2. **Mise en réseau après la sécurité.** Les professionnels de la mise en réseau opèreront en suivant les politiques ZTE définies par l'équipe de sécurité. Bien que cet arrangement fasse progresser de manière significative l'idéologie de Zero Trust, il bouleverse le principe des 25 dernières années qui consistait à superposer la sécurité sur la mise en réseau.

3. **Enfin, un accès plus sûr à Internet.** Les concepteurs à l'origine d'Internet admettent volontiers que la sécurité n'a jamais fait partie de leur projet. Dans les 30 ans qui ont suivi sa création, l'Internet mondial est devenu un réseau dangereux à parcourir. La technologie Zero Trust Edge offre enfin un accès plus sûr.

Autres ressources

Entreprises interrogées pour ce rapport

Nous tenons à remercier les personnes des entreprises suivantes, qui ont généreusement donné leur temps pour la recherche dans le cadre de ce rapport.

419 Consulting
Akamai
AT&T
Axis Security
Barracuda
BlackBerry

Cato Networks
Cisco Systems
Citrix
Deutsche Telekom
Edelweiss Financial Services
Famous Supply
Fortinet
Infoblox
IronNet
Jefferies
Juniper
Lightstream
Marriott Vacations Worldwide
Menlo Security
Mentor Graphics
Netskope
Nuspire
Palo Alto Networks
Silver Peak
SKF
VMware
Windstream
Zentera Systems
Zscaler

Notes de fin

[1] Un datacenter privé constitue la plate-forme des données, des applications et de la sécurité en lien avec des sites distants. Les restaurants, les centres de soins actifs, les sites de fabrication, pour n'en citer que quelques-uns, se connectent à la plate-forme pour toutes les ressources de l'entreprise.

[2] Voir le rapport Forrester « Emerging Technology Spotlight: BusinessWide Networking Fabric » (Eclairage sur la technologie émergente : la structure réseau à l'échelle de l'entreprise).

Dans un modèle d'entreprise en réseau, les membres de l'écosystème co-créent une valeur client de manière distribuée. Voir le rapport Forrester « Customer-Obsessed Businesses Need Digital Ecosystems » (Les entreprises centrées sur le client ont besoin d'écosystèmes numériques).

[3] Dans nos enquêtes sur l'expérience pandémique (PandemicEX), nous avons posé la question suivante : « Dans quelle mesure votre entreprise/organisation suit-elle ces étapes pour gérer le risque associé au coronavirus ? » Source : première enquête Forrester « PandemicEX » du premier trimestre 2020 (3 au 6 mars 2020) ; deuxième enquête Forrester « PandemicEX » du premier trimestre 2020 (17 au 19 mars 2020) ; et première enquête Forrester « PandemicEX » du deuxième trimestre 2020 (1er au 3 avril 2020).

Voir le rapport Forrester « The State Of Remote Work, 2020 » (Etat des lieux du télétravail en 2020).

[4] Les supports marketing des fournisseurs au début du lancement du ZT ne mettent en évidence que les solutions pour les datacenters privés. Par exemple, Palo Alto a souligné dans divers livres blancs comment le ZT peut protéger les actifs du datacenter. Source : « Best Practices - Data Center Security », Palo Alto Networks, 1er juin 2016 (https://www.paloaltonetworks.com/resources/whitepapers/best-practices-data-center-security).

[5] Source : Sushant Jain, Alok Kumar, Subhasree Mandal, Joon Ong, Leon Poutievski, Arjun Singh, Subbaiah Venkata, Jim Wanderer, Junlan Zhou, Min Zhu, Jonathan Zolla, Urs Hölzle, Stephen Stuart, et Amin Vahdat, « B4: Experience with a Globally-Deployed Software Defined WAN », compte-rendu de la conférence ACM SIGCOMM 2013, août 2013 (https://storage.googleapis.com/pub-tools-public-publication-data/pdf/41761.pdf).

FORRESTER®

Nous travaillons avec des responsables technologiques et commerciaux pour développer des stratégies centrées sur le client qui stimulent la croissance.

PRODUITS ET SERVICES

- Recherche fondamentale et outils
- Données et analyses
- Collaboration entre pairs
- Mission des analystes
- Conseil
- Evénements

Les recherches et les analyses de Forrester sont adaptées à votre rôle et aux initiatives stratégiques de l'entreprise.

LES RÔLES AUXQUELS NOUS RÉPONDONS

Professionnels du marketing et de la stratégie

Directeur marketing (CMO)
Marketing B2B
Marketing B2C
Expérience client
Informations client
Commerce électronique et stratégie de distribution

Professionnels de la gestion des technologies

DSI
Développement et distribution d'applications
Architecture d'entreprise
Infrastructure et opérations
- Sécurité et gestion des risques

Gestion de l'approvisionnement et des fournisseurs

Professionnels de l'industrie technologique

Relations avec les analystes

SUPPORT CLIENT

Pour en savoir plus sur les réimpressions papier ou électroniques, contactez le support client au +1 866-367-7378, au +1 617-613-5730 ou à l'adresse clientsupport@forrester.com. Nous proposons des remises sur volume et des tarifs spéciaux aux établissements d'enseignement et aux organismes à but non lucratif.

161728