APIXIT

L'expertise augmentée

Le secure SD-WAN : un réseau intelligent et sécurisé, adapté à vos problématiques métiers d'aujourd'hui et de demain

LIVRE BLANC Avril 2019

cisco Meraki

SOMMAIRE

QUI SOMMES-NOUS ?

APIXIT

APIXIT est l'union des deux spécialistes indépendants des services numériques DCI et RETIS. Expert reconnu des solutions d'infrastructures digitales, de la Digital Workplace, de la Cybersécurité, APIXIT propose un accompagnement global : audit, conseil, intégration en mode projet, services managés. Conscient que l'Innovation est une attente des clients et un atout différenciant, APIXIT est le partenaire privilégié des plus grands constructeurs et éditeurs et porte son attention et son expertise sur les enjeux des organisations et de la transformation digitale.

Animé par une solide culture de la performance, de l'innovation technologique et de la satisfaction client, le groupe APIXIT et ses 350 collaborateurs sont présents à travers toute la France.

CISCO MERAKI

Fondée en 2006, Cisco Meraki est une entreprise leader du monde informatique avec plus de 350 000 clients et 4.5 millions d'appareils connectés dans le monde. Les produits Cisco Meraki offrentaux administrateurs une visibilité complète du réseau depuis une interface intuitive, sans les coûts et complexités associés aux architectures traditionnelles. La gamme complète de solutions Meraki comprend des bornes WiFi, switches, appareils de sécurité, caméras de surveillance ainsi qu'une solution de gestion de flotte mobile. La technologie SD-WAN est intégrée à tous les appareils de sécurité, permettant de réduire les coûts d'exploitation pour les déploiements multi-sites et de garantir les meilleurs niveaux de performance.

CONTACTS

Jean-Philippe GUILLEMIN
Responsable développement d'activité Cybersécurité
jpguillemin@apixit.fr
Tél : 02 99 06 37 02

Céline SALOT
Chargée de Marketing
csalot@apixit.fr
Tél : 02 99 06 31 83

Ces dernières années, les usages du numérique en entreprise ont considérablement évolué. Beaucoup d'organisations effectuent actuellement leur mue digitale. Si on a généralement tendance à penser que cette transformation numérique s'exprime au travers de l'aménagement des espaces de travail et de l'usage au quotidien de solutions digitales (écrans tactiles et projection, partage documentaire, équipements de visioconférence et de collaboration…) ; on oublie parfois qu'elle a aussi un impact sur les infrastructures et le niveau de sécurité des organisations.

Face aux nouveaux enjeux auxquels font face les organisations, les DSI doivent relever le défi d'une infrastructure IT efficiente au service des utilisateurs et de leur organisation. Si les réseaux traditionnels privés ne semblent plus répondre intégralement aux enjeux d'agilité, de sécurité et de coût des entreprises, les solutions secure SD-WAN présentent, elles, des atouts qui séduisent de nombreux responsables informatiques.

25%

des entreprises
vont passer au SD-WAN
dans les 2 ans à venir.

Source : Gartner

x2

Le chiffre d'affaire du SD-WAN
va presque doubler tous les ans
jusqu'en 2020.

Source : IDC France

UNE ÉVOLUTION DES INFRASTRUCTURES IT POUSSÉE PAR DES NOUVEAUX BESOINS EN ENTREPRISE

Les exigences des professionnels en matière de réseau privé d'entreprise ont considérablement évolué ces dernières années. Elles sont le fruit d'une profonde mutation de nos méthodes et de nos outils de travail.

Trois facteurs majeurs expliquent les besoins nouveaux des entreprises en matière de réseau :

- La digitalisation des organisations
- Une plus grande mobilité des collaborateurs
- Un recours de plus en plus courant aux services hébergés dans le cloud

Les usages digitaux se développent et se démocratisent

Même s'il existe de grandes disparités en termes de maturité digitale selon les organisations, les équipes dirigeantes des entreprises s'accordent à penser que la transformation digitale de leurs activités est un prérequis pour améliorer leur efficience et garantir leur pérennité. Les projets de digitalisation et de dématérialisation des activités sont donc lancés dans de nombreuses organisations.

76%

des dirigeants considèrent que la transformation digitale de leur organisation est un sujet stratégique

Source : Umanis, juin 2017

Poussé notamment par l'émergence des nouvelles technologies numériques et par l'arrivée sur le marché du travail des digitals natives, l'usage quotidien d'écrans tactiles, de bornes, de tablettes. se démocratise. La communication interne comme externe à l'entreprise s'effectue de plus en plus via des canaux digitaux. On utilise, par exemple, des solutions digitales pour de la gestion de projet, des réunions de créativité, des sessions de formation ou pour suivre, via des indicateurs prédéfinis, l'activité des différents services et sites des organisations.

En magasin et en agence commerciale, tout est mis en place pour faire vivre aux clients une expérience d'achat unique grâce à une approche personnalisée et omnicanal. La frontière entre l'espace commercial physique et virtuel s'estompe. Les visiteurs peuvent commander en ligne leurs achats et les récupérer en magasin ou au contraire choisir de se faire livrer, on met à leur disposition des bornes et écrans qui leur permettent de commander des services supplémentaires, de comparer et de noter des produits et services, de se repérer plus facilement dans les espaces de vente, de s'informer sur les produits et services vendus, d'adhérer à des programmes de fidélisation… Beaucoup d'applications sont également créées pour accompagner les collaborateurs et les clients, les informer et simplifier leurs usages.

Les métiers sont donc régulièrement demandeurs de nouveaux services et amènent de nouveaux usages. Ainsi, les volumes de données générés et partagés explosent et imposent aux organisations de faire évoluer leurs infrastructures digitales et leurs mesures de sécurité.

90%

des données mondiales ont été créées au cours des deux dernières années.

Source : IBM, janvier 2018

Dans un tel contexte, les services informatiques doivent être en mesure d'assurer une qualité de service du réseau irréprochable, sans souci de performance ou de disponibilité.

Les diffusions vidéo ne peuvent souffrir de problématiques de latence par exemple. Il faut également s'assurer que l'infrastructure WAN en place ait la capacité d'absorber les besoins supplémentaires en bande passante induits par les nouveaux usages numériques des métiers ; et qu'elle soit simplement administrable pour optimiser les temps de mise à disposition des services aux métiers.

28%

Les besoins en bande passante des entreprises augmentent chaque année, en moyenne de 28% tandis que ceux consacrés à la connectivité WAN restent stables.

Source : Gartner, 2015

Une population active toujours plus mobile

Une étude menée par Forester Research indique que 60% des salariés travaillent sur plusieurs sites pendant la semaine. Que ce soit chez un client, un partenaire, en télétravail ou depuis un tiers lieu quelconque, on observe depuis quelques années une augmentation de la pratique du travail nomade. Jamais la frontière entre l'espace domestique et l'espace de travail n'a été si fine. Les implantations géographiques des organisations sont morcelées pour répondre à des enjeux de réactivité et de flexibilité. Aussi, de nombreuses solutions de connectivité sont mises en place dans les organisations pour permettre aux collaborateurs de travailler sans difficulté et en toute sécurité qu'importe le lieu où ils se trouvent. Grâce, notamment, aux solutions de connexion à distance, aux applications hébergées, et au développement de services de collaboration intégrés, l'espace de travail se dématérialise.

Ces nouveaux modes d'organisation révolutionnent le quotidien des entreprises et la façon dont elles doivent concevoir leur système d'information. En effet, tout doit être mis en œuvre pour que le nomadisme ne créé pas de barrières entre les collaborateurs et de freins dans la réalisation de leurs activités quotidiennes. L'infrastructure réseau doit être conçue de telle sorte à faciliter l'accès aux données de l'entreprise pour les collaborateurs nomades et ceux basés sur un site distant, tout en prenant en compte les divers équipements utilisés (pc, tablette, smartphone, objet connecté). Une connexion sécurisée établie avec le terminal de l'utilisateur doit lui permettre de se connecter au système d'information et aux applications utilisées par l'entreprise via toute type d'accès réseau (Wifi, réseau mobile….).

Des mesures spécifiques doivent, en outre, être prises pour protéger le patrimoine informationnel des organisations dans un contexte de nomadisme accru : une gestion stricte des identités, une politique de sécurité du système d'information (PSSI) adaptée à ces nouveaux enjeux, des accès à distance contrôlés, le chiffrement des flux d'information, une sensibilisation régulière des collaborateurs aux bonnes pratiques en matière de cybersécurité…

Un recours au cloud généralisé

Parce qu'il offre aux collaborateurs la possibilité de travailler simplement sur des dossiers communs et d'échanger à distance ; le modèle Cloud est plébiscité par de nombreux professionnels. Outre le fait qu'il réponde à des enjeux de mobilité importants, les organisations, séduites par les caractéristiques du modèle *as a service* (fonctionnalités évoluées, administration déléguée, haute disponibilité garantie, modèle financier OPEX,…), sont nombreuses à mettre en place une stratégie « Cloud-first » au sein de leur organisation. Il est désormais courant d'utiliser des messageries (via Office365 ou Google Apps), des espaces de stockages collaboratifs ou des plateformes de services (par exemple Salesforce) hébergés.

70% → **96%**

70% des entreprises aujourd'hui et 96% dans deux ans auront 50% de leurs applications hébergées dans le Cloud.

Source : Globbsecurity, février 2018

x3

L'usage actuel du Cloud est près de 3 fois supérieur à ce qu'il était il y a 4 ans.

Source : IDG

Les directions informatiques doivent impérativement repenser le fonctionnement et l'architecture de leur WAN dans cette optique « cloud first ». La migration des applications business vers le cloud étant bien engagée, l'infrastructure réseau doit être en mesure d'absorber les besoins supplémentaires en bande passante induits. Il est également primordial qu'elle puisse garantir aux utilisateurs une connectivité optimale et un niveau de performance et de sécurité du réseau élevé. Les responsables informatiques pourront, pour ce faire, s'appuyer sur des technologies innovantes qui leur permettent de prioriser dynamiquement leur trafic et de créer des liens directs entre les sites distants de l'entreprise et internet, sans nécessairement passer par le datacenter.

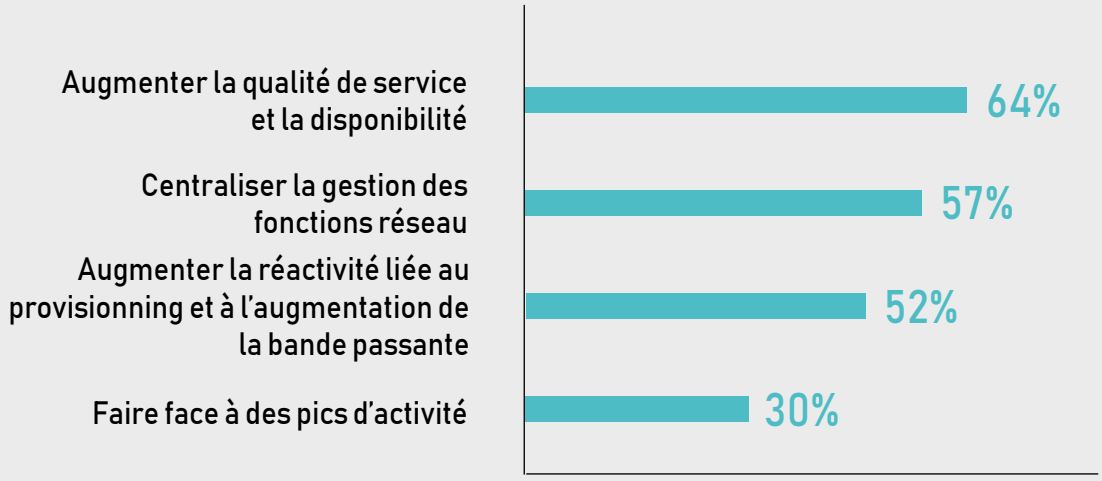
Des enjeux de sécurité inhérents aux nouveaux usages digitaux

Dans ce contexte nouveau, des mesures particulières devront être engagées pour garantir la sécurité du réseau et des données de votre organisation. De nouvelles menaces et de nouveaux risques apparaissent à mesure que vos usages IT évoluent. Une prise de conscience de la part des organisations et des salariés est nécessaire pour assurer un bon niveau de protection des données et réseaux. Cet enjeu est d'autant plus important que les conséquences légales, économiques et en termes d'image peuvent être dévastatrices pour les organisations qui seraient touchées par un incident grave de sécurité. Aussi, il semble essentiel de bien intégrer une dimension sécuritaire à votre démarche SD-WAN. C'est pourquoi, nous parlons dans ce livre blanc de secure SD-WAN, et non pas uniquement de SD-WAN.

STATISTIQUES

Les motivations qui poussent les organisations à migrer leur infrastructure vers une solution secure SD-WAN :

Les solutions secure SD-WAN se présentent aux yeux de nombreux décideurs informatiques comme la réponse technologique qui leur permettra d'adapter leur infrastructure réseau aux nouvelles attentes des métiers.

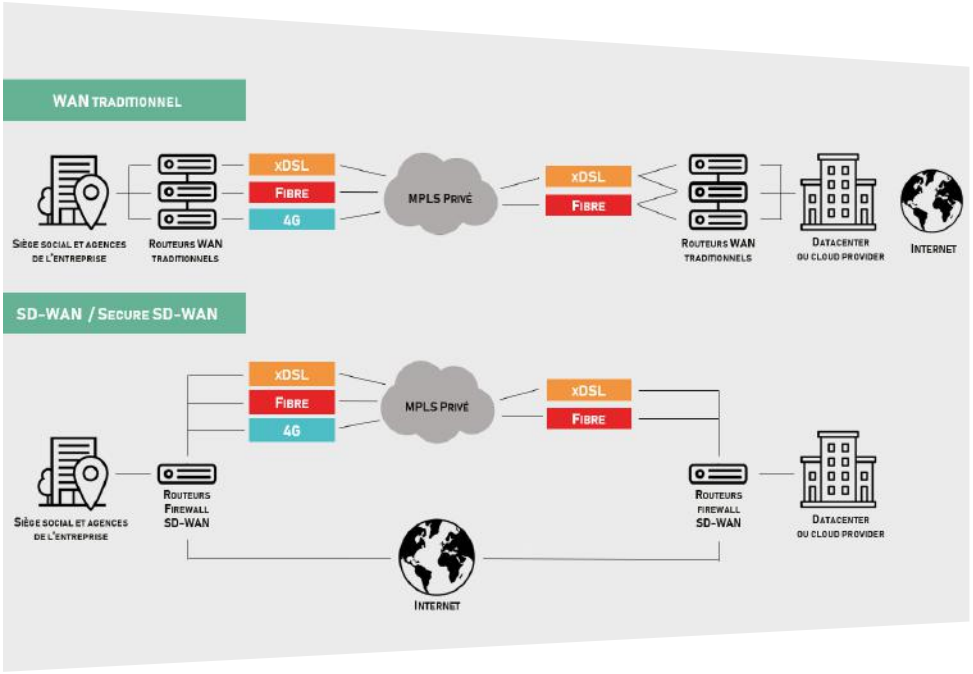


Source : IDC France, septembre 2016

LE SECURE SD-WAN : CARACTÉRISTIQUES ET ATOUTS

Le SD-WAN (Software defined wide area network, en français « réseau étendu à définition logicielle) est considéré comme une innovation majeure en termes de réseaux privés d'entreprises. Il s'agit de la troisième génération de réseaux privés étendus après les technologies IPsec (internet protocol security) et MPLS (multi protocol label switching).

Basées sur un socle logiciel, les infrastructures secure SD-WAN vous permettent de sécuriser et d'orchestrer simplement et en continu des réseaux privés étendus et des accès internet. Vous avez la capacité d'intégrer dans votre infrastructure WAN des liaisons d'accès de toute nature (ADSL, SDSL, Fibre optique, 4G, MPLS…) et de faire transiter vos flux vers les liens les plus adaptés. L'aiguillage des flux s'effectue dynamiquement en fonction des règles que vous aurez prédéfinies. Les différents sites de votre organisation peuvent, en outre, disposer de leur propre capacité de routage. Il n'est plus nécessaire de faire transiter les flux de vos sites distants par votre site principal.



Du WAN traditionnel au secure SD-WAN

Une évolution de votre architecture réseau et un aiguillage dynamique de vos flux selon des règles définies en amont prenant en compte les problématiques de sécurité, de coût et de performance de votre organisation.

La technologie secure SD-WAN suscite un engouement particulier auprès des directions des systèmes d'information. Par ses caractéristiques intrinsèques, elle répond particulièrement aux enjeux de transformation actuels des organisations.

61% des entreprises interrogées envisagent un déploiement SDN axé sur le WAN dans les 2 années à venir.

Source : IDC, forecast 2017-2021

Une gestion des liens rationalisée pour une bande passante optimisée

Les solutions secure SD-WAN vous permettent d'optimiser significativement l'usage de votre bande passante grâce à une meilleure gestion de vos liens. En effet, vous avez la possibilité d'agréger au sein de votre infrastructure réseau des liens de différentes natures et de router dynamiquement vos flux selon le type de lien et leur disponibilité. Avec le secure SD-WAN, le routage de vos flux est totalement repensé ; il va bien au-delà d'un simple transfert de paquets d'un point A à un point B. Vos flux sont désormais aiguillés de telle sorte à garantir la sécurité et la performance de vos applications. Contrairement à un routage dit « traditionnel » qui opère un partage de charges simple et gère vos liens selon un mode actif/passif, le routage de type SD-WAN vous permet d'orienter intelligemment le trafic sur vos différents liens en tenant compte de leur utilisation réelle.

28%

des entreprises, seulement, utilisent une solution d'accélaration ou de priorisation des flux.

Source : IDC France, septembre 2016

Grâce à une analyse plus poussée des flux passant dans votre réseau (inspection profonde des paquets (IPD) ou deep paquet inspection (DPI) en anglais), vous avez la capacité de prioriser vos flux en fonction de la criticité de vos activités. Vous garantissez ainsi une qualité de service élevée à l'ensemble de vos utilisateurs.

74% des entreprises assimilent la dégradation des performances du réseau WAN comme une baisse de productivité.

Source : IDC France, septembre 2016

Une optimisation de vos débits

Avec une démocratisation des usages numériques et un recours plus fréquent aux applications hébergées, les besoins en bande passante des entreprises explosent. Alors que votre DSI aurait naturellement investi dans de nouvelles liaisons pour répondre à un besoin croissant; une solution SD-WAN vous permet, en premier lieu, d'optimiser l'utilisation de vos débit existant. Dans une infrastructure SD-WAN, la bande passante de chacun de vos liens est mutualisée. Selon les règles de routage que vous aurez prédéfinies, lorsque la bande passante d'un lien sera totalement utilisée, vos flux seront automatiquement redirigés vers un autre lien de votre réseau. Dans cette logique, vous n'avez pas de liens « encombrés » ou, a contrario, de liens sous utilisés. Le fonctionnement de votre réseau est fluide et vous optimisez le dimensionnement de votre réseau en fonction de vos flux réels.

Grâce à une meilleure visibilité de votre trafic, vous avez également la possibilité de priorisez vos flux business critiques par rapport à du trafic « récréatif ». Cela constitue un levier supplémentaire d'optimisation de vos débits. Si vous jugez que l'ensemble de votre trafic est critique pour votre organisation, vous vous orienterez alors vers une augmentation de votre débit global avec la possibilité de mettre en place des connexions directes vers vos applications *as a service*.

42%

des entreprises considèrent que la qualité de service de leur réseau est insuffisante.

Source : IDC France, Septembre 2016

1/3

des entreprises jugent le délai nécessaire à l'augmentation du débit ou à l'ajout d'un lien trop long.

Source : IDC France, Septembre 2016

Une baisse de vos coûts de fonctionnement

Grâce à la mutualisation des liens, la priorisation et le routage dynamique de vos flux, les solutions secure SD-WAN vous permettent de réduire substantiellement les coûts associés au fonctionnement de votre réseau. Outre les économies relatives à l'optimisation de vos débits, vous avez la possibilité d'associer à vos liaisons WAN traditionnelles (liaisons MPLS-VPN), des connexions internet beaucoup moins coûteuses. Cette infrastructure WAN hybride vous permettra alors de continuer à router vos flux critiques sur vos liaisons WAN privées et d'orienter désormais vos autres applications vers vos liens internet. Votre trafic transite via le lien le plus adapté (en fonction de vos enjeux de performance et de sécurité), le tout à coût maitrisé. Ces affectations étant réalisées dynamiquement grâce aux règles édictées en amont via le portail d'administration du réseau, vous n'avez plus besoin de solliciter continuellement un administrateur réseau. Vous réalisez ainsi des économies de « temps-Homme » non négligeables.

Une intéropérabilité cloud augmentée

Les solutions secure SD-WAN favorisent les interactions avec vos différents services hébergés dans le cloud. Grâce à la virtualisation de l'infrastructure, il est très simple de s'interconnecter avec des cloud privés et publics. Le réseau local de votre organisation s'étend très simplement à tous vos services tiers et sites distants à travers le monde. Vous pouvez accéder à vos applications hébergées sans repasser nécessairement par votre site principal grâce à des connexions internet en accès direct ; le tout de façon totalement sécurisée grâce à la tunnelisation des connexions. Ces accès directs permettent, en outre, de dé-saturer le trafic de vos liens opérateurs centraux.

D’avantage d’agilité pour les sites distants de votre organisation

Actuellement, une grande majorité des entreprises multi-sites utilisent des VPN (virtual private network ou réseaux privés virtuels : VPN IPsec, VPN SSL, MPLS…) pour faire communiquer leurs différents sites entre eux. Des solutions de routage de flux sont installées sur chaque site distant pour orienter le trafic. Avec une solution secure SD-WAN, il n’est plus nécessaire de mettre en place ces routeurs. Il vous suffit de paramétrer des Appliances SD-WAN (ou des routeurs virtualisés, tels que des optimiseurs WAN) pour doter vos sites distants de capacités de routage locales.

Comme évoqué précédemment, vous avez également la possibilité de créer des liaisons directes entre vos sites distants et vos services hébergés ou le datacenter de votre organisation grâce à des connexions tunnelisées. Votre infrastructure SD-WAN étant totalement administrable depuis un contrôleur central, il vous sera simple et rapide d’homogénéiser vos paramétrages réseau pour l’ensemble de vos implantations.

Une politique de gestion et de sécurité centralisée et homogène

L’ensemble de votre infrastructure réseau secure SD-WAN repose sur un contrôleur central sur lequel est adossé une interface d’administration. Intuitive et simple d’utilisation, cette interface doit vous permettre d’avoir plus de visibilité et de mieux contrôler les différents paramétrages de votre réseau et vos équipements. Compte tenu de la multiplicité et de l’hétérogénéité des liens qui constituent votre réseau, avoir une interface unique de gestion devient primordial pour assurer un niveau de performance élevé et une sécurité de bout en bout de votre réseau.

Cela vous permet d’administrer au quotidien (règles de gestion, routage, priorisation des flux…) et de façon homogène, l’ensemble de vos sites en France ou à l’étranger, et ce même s’ils sont reliés à différents opérateurs. Grâce au monitoring de l’activité de votre réseau depuis cette plateforme, vous pouvez réajuster dès qu’il est nécessaire vos paramétrages et agir de manière proactive sur votre niveau de sécurité. Ainsi, votre infrastructure évolue à mesure que les usages de vos utilisateurs et les besoins de votre organisation changent.

Un gain de temps précieux pour les DSI

Le routage dynamique des flux, la gestion intelligente des liens et l'administration centralisée de votre réseau constituent le socle du réseau intelligent de demain. Alors qu'auparavant, il fallait paramétrer l'ensemble des liens et effectuer en permanence des ajustements sur le réseau MPLS en tenant compte des besoins utilisateurs et des équipements hétéroclites ; beaucoup de tâches sont désormais automatisées.

Le secure SD-WAN vous permet une gestion WAN optimisée avec un temps d'administration limité. Vos équipes IT n'ont plus à se concentrer sur des tâches d'administration du réseau parfois fastidieuses et rébarbatives. Elles peuvent se recentrer sur des activités créatrices de valeur pour l'entreprise. Grâce à l'automatisation de la gestion du WAN, vous limitez les temps de paramétrage et réduisez ainsi l'impatience de vos utilisateurs et le coût d'administration de votre infrastructure.

7 ÉTAPES À SUIVRE POUR UNE MIGRATION SECURE-SD-WAN RÉUSSIE

Faire évoluer son infrastructure réseau traditionnelle vers une solution secured SD-WAN n'est pas une tâche anodine. Il est essentiel de bien préparer la migration de votre réseau privé. Les équipes IT en charge du déploiement SD-WAN devront parfaitement identifier les enjeux du projet en amont afin d'offrir des performances optimales aux utilisateurs et de définir des règles en cohérence avec la politique de sécurité de l'entreprise. Il faudra également veiller, lors de la phase de déploiement du réseau, à ce que les activités quotidiennes de l'entreprise ne soient pas perturbées.

1%
des entreprises étaient équipées de SD-WAN en 2017.
Source : Gartner 2017

30%
d'entre-elles le seront à l'horizon 2020.
Source : Gartner, 2017

Pour cela, nous vous recommandons de suivre les étapes détaillées ci-dessous.

Etape 1
Audit des flux et de l'infrastructure existante

Avant d'initier toute démarche de transformation, il est primordial de faire un audit complet de votre infrastructure réseau existante. Cette phase d'ingénierie joue un rôle essentiel dans la réussite de votre projet de migration. Elle doit vous permettre d'acquérir une compréhension poussée des modèles et des flux de trafic, des applications utilisées et des activités qui s'y rattachent. C'est à cette étape du projet qu'il vous faut établir une cartographie précise de votre réseau permettant d'identifier chaque lien disponible et de préciser la façon dont ils sont administrés et sécurisés. Le mapping réalisé vous donnera une vue claire de la façon dont tous les composants de votre réseau sont interreliés, du niveau d'utilisation de vos applications et protocoles et ainsi de la bande passante disponible. L'ensemble des informations collectées vous aiderons à préciser vos besoins et à identifier les points critiques du projet de migration.

Etape 2
Définition des besoins et identification des enjeux critiques du projet

L'analyse du WAN existant effectuée lors de la phase précédente vous permet de mettre en évidence les liens présentant des instabilités et les activités soumises à des vulnérabilités ou des baisses de performance.

Ce sont ces éléments que vous pourrez corriger et optimiser dans la nouvelle infrastructure réseau. Cette analyse technique doit cependant être couplée à un audit des besoins fonctionnels des utilisateurs. Il faudra tenir compte des attentes quotidiennes des métiers en identifiant les applications critiques dont la disponibilité et la performance devront être garanties, et préciser les besoins des métiers en bande passante. En effet, un service marketing qui communique via des supports vidéo aura, par exemple, un besoin de bande passante plus important que pour un affichage digital simple, pour assurer la diffusion du flux vidéo sans coupure. A l'issue de ces deux audits, grâce à une meilleure connaissance de vos activités, vous serez en mesure d'optimiser l'administration de votre réseau et d'envisager, si besoin, une augmentation de bande passante.

Etape 3
Conception et maquettage de la nouvelle infrastructure

Une fois que les attentes liées à votre architecture réseau sont bien identifiées, vous pouvez maquetter votre nouvelle infrastructure. Il ne s'agit pas là simplement, de superposer plusieurs connexions de technologies différentes. Vous devez choisir judicieusement vos lignes d'accès en prenant en compte votre besoin et la qualité, la capacité et le coût de chaque technologie. Votre équipe informatique devra également catégoriser les applications du réseau en fonction des retours terrain précédents, leur affecter une priorité adaptée et définir une politique de routage. Une fois tout ce travail effectué, vous devez aboutir à une nouvelle cartographie des applications et des flux de connectivité de votre entreprise en capacité de supporter les usages business quotidiens de l'ensemble des collaborateurs. Dans le cadre d'une migration partielle de votre réseau, vous devrez également anticiper la façon dont votre infrastructure SD-WAN s'intègrera avec votre infrastructure actuelle.

Etape 4
Déploiement pilote de votre nouvelle infrastructure WAN

Nous préconisons, avant une implémentation à grande échelle de l'infrastructure SD-WAN conçue sur plan, d'effectuer un déploiement pilote sur une partie restreinte de votre réseau. Procéder de cette façon permet de valider et d'éprouver la conception établie lors des étapes précédentes du projet de migration. Le déploiement pilote est un bon moyen de sécuriser votre démarche. Sur un périmètre restreint, vous limitez les impacts négatifs potentiels de votre changement technologique sur les activités créatrices de valeur de votre organisation. Même si vous pourrez contrôler point par point le bon fonctionnement de votre nouvelle infrastructure lors de la phase de recette, la migration d'une partie pilote de votre infrastructure vous permet de vérifier que la bande passante disponible est allouée selon les politiques prédéterminées et avec un niveau de sécurité conforme aux exigences fixées par la politique de sécurité de l'organisation. Vous pourrez identifier les aspects complexes du déploiement et ainsi éviter certains écueils lors du déploiement industriel du nouveau réseau privé d'entreprise. C'est également durant cette phase que les utilisateurs pilotes pourront faire leurs retours-terrain et soumettre des suggestions d'amélioration.

Etape 5
Déploiement industriel de la nouvelle infrastructure réseau

Après avoir effectué les ajustements qui s'imposaient au vu du déploiement pilote de la solution secure SD-WAN, il est temps de passer à la phase de déploiement industriel. Même si le pilote a été riche en enseignements, le déploiement de la nouvelle infrastructure, socle technologique de l'ensemble des activités de l'entreprise, n'en reste pas moins critique et complexe. Chaque site doit pouvoir être migré sans perturber le quotidien des collaborateurs. Pendant l'implémentation de la nouvelle solution réseau, il faudra veiller à ce que l'infrastructure traditionnelle puisse communiquer avec les sites déjà migrés en SD-WAN.

Etape 6
Tests et recette

Lorsque le déploiement de la nouvelle architecture est achevé, il convient de vérifier point par point que l'installation mise en place réponde bien au cahier des charges qui avait été défini en amont et surtout aux attentes des utilisateurs et des administrateurs du réseau. Les tests unitaires réalisés permettront de s'assurer que le comportement des flux de données est conforme aux politiques de sécurité fixées par l'organisation et respecte les priorités de routage déterminées. Le recettage est également l'occasion de collecter les retours des utilisateurs et de voir comment la nouvelle infrastructure réseau réagit lorsqu'elle est soumise à un flux important de données ou à des enjeux de sécurité particuliers. Au terme de cette phase, l'ensemble des collaborateurs bénéficieront au quotidien d'une expérience de travail optimale grâce à un socle réseau performant et totalement paramétré pour répondre à leurs besoins.

Etape 7
Monitoring et supervision du réseau

Si votre projet de migration vers une solution secure SD-WAN touche à sa fin une fois le recettage de la nouvelle architecture WAN achevé, il ne faut pas pour autant considérer vos problématiques réseaux comme un sujet clôt. Il est essentiel de mettre en place un système de monitoring continu du réseau. En effet, les besoins de vos utilisateurs peuvent être amenés à évoluer et aucun réseau n'est à l'abri d'un incident de sécurité. Vous devez donc veiller à ce que votre infrastructure réponde toujours aux objectifs que vous vous êtes fixés (connexion réseau performante, optimisation des politiques de routage, ...) et qu'elle protège bien le capital informationnel de votre organisation. La visibilité apportée par la supervision de votre réseau vous permettra de réagir au plus vite en cas de cyber-attaque.

REGARD D'EXPERT

La cybersécurité, l'incontournable de vos infrastructures SD-WAN !

— Par Nicolas Henaine

Avec les solutions SD-WAN, les entreprises optimisent l'utilisation du WAN. Cette optimisation passe généralsement par la migration des liens WAN MPLS vers une solution hybride MPLS/Internet pour l'ensemble de sites.

De ce fait, il est important d'intégrer toutes les notions de sécurité au sein des réflexions SD-WAN. L'utilisation d'un lien internet en local intègre :

— une solution de sortie internet sur chaque site
— un besoin de sécurisation avancé des flux et des données pour chaque site

Ces deux aspects obligent les organisations à déployer des services de sécurité pour chaque site distant. Ceci permet de répondre aux exigences de la politique de sécurité globale de l'entreprise.

Avec les solutions Secure SD-WAN, l'ensemble des fonctionnalités avancées sont présentes au sein d'un seul équipement gérant à la fois :

— le SD-WAN
— La sécurité périmétrique du site
— L'ensemble des services de sécurité avancés de manière centralisée et homogène pour l'ensemble des sites (IDS/IPS, Filtrage URL, Antivirus, Filtrage Applicatif,...).

Contrairement à une approche secure SD-WAN, le SD-WAN implique l'ajout d'une brique de sécurité. Cela complexifie l'architecture locale et la gestion au quotidien du réseau et augmente les coûts de maintien en conditions de sécurité de l'ensemble de sites de l'entreprise. Avec l'approche secure SD-WAN, la sécurité est intégrée automatiquement dans la gestion dynamique des flux. Elle est gérée de bout-en-bout, intégrant l'ensemble de la chaîne de service, du réseau local au réseau Datacenter en passant par le WAN.

« Plus d'un tiers des entreprises ont subi une attaque de sévérité importante à critique sur le second semestre 2017 »

— Rapport cybersécurité, Fortinet, 2018

Avec le secure SD-WAN, plus de concession à faire entre performance et coûts. Les entreprises bénéficient d'une connexion haut débit abordable. Elles peuvent chiffrer l'ensemble du trafic envoyé depuis et vers chaque site distant. Cela peut se faire sans que l'administrateur réseau ne doive modifier manuellement la configuration de chaque routeur au moindre changement apporté au réseau.

Bibliographie

- Le SDN appliqué au WAN en France, IDC France, septembre 2016
- Gartner Market Guide for WAN Edge Infrastructures, Gartner, 2017
- Le SD-WAN pour les nuls, Jérôme Durand, Cisco Systems, 2017
- SD-WAN : comment éviter les problèmes de déploiement en 10 points clés ? Solutions numériques, août 2017
- SD-WAN : conseils pour un déploiement simple ! News Informatique, avril 2018
- Sécurité SD-WAN : quels impératifs ? ITPro, octobre 2018
- SD-WAN : les entreprises françaises multiplient les POC, Le monde Informatique, 2017
- SD-WAN, cette technologie clé qui déporte l'entreprise sur plusieurs sites, Global Security Mag, septembre 2018
- Explosion en vue pour le marché du SD-WAN, silicon, mars 2016

APIXIT

L'expertise augmentée

Ce Livre Blanc est un document d'information rédigé par la société APIXIT.
Il n'a pas vocation à servir de support de prestation de conseil.

SIEGE SOCIAL

Les Conquérants
Immeuble Annapurna
1 avenue de l'Atlantique
91940 LES ULIS

RENNES

Espace Jacques Cartier
CS 96031
35360 MONTAUBAN
DE BRETAGNE

LILLE

Village Créatif
10 rue de la Cense
59650 VILLENEUVE D'ASCQ

QUIMPER

3 allée Emile Le Page
29000 QUIMPER

PARIS

Immeuble AXIUM
22/24 rue du Gouverneur
Général Félix Eboué
92130 ISSY LES MOULINEAUX

NANTES

Les Espaces Océane
4 rue Jack London
44400 REZÉ

REIMS

13 rue Desbureaux
51100 REIMS

TOULOUSE

2 rue des Cosmonautes
31400 TOULOUSE

478 rue de la découverte Mini
Parc 3 - CS 67624
31676 LABEGE Cedex

LYON

Immeuble Woodclub
97, allée Alexandre Borodine
69800 SAINT-PRIEST

5D chemin du Jubin
69570 DARDILLY

www.apixit.fr