

STORMSHIELD

SD-WAN de confiance : allier performance et sécurité

Octobre 2022

Table des matières

04

Implémentation du SD-WAN, pourquoi est-elle indispensable ?

07

La menace cyber des États-nations

11

SD-WAN : **amélioration** de l'expérience applicative

14

SD-WAN : **adaptabilité** pour les différents usages

17

La nécessaire sécurisation des communications

20

La gestion efficace du SD-WAN

23

Trusted SD-WAN : **le choix de confiance**

27

Trusted SD-WAN by Stormshield : **confiance et sécurité tout-en-un**

Les organisations ont enclenché des changements structurels et numériques proposant une meilleure expérience pour leurs collaborateurs et clients ainsi que des améliorations dans leurs processus informatiques.

Dans ce cadre, le Software Defined Wide Area Network ou SD-WAN trouve sa place dans la nécessaire transformation numérique des entreprises car cette technologie simplifie la gestion des réseaux sur les différents sites tout en optimisant les coûts.

Cette approche est un moyen innovant d'améliorer la performance et d'unifier la connectivité des différents réseaux, incluant le cloud hybride. Le SD-WAN permet aux entreprises d'**adapter dynamiquement le trafic Internet** selon leurs besoins de priorité et de qualité de bande passante sur chaque emplacement.

Néanmoins, pour obtenir une meilleure protection de votre infrastructure, **la technologie SD-WAN se doit d'être sécurisée et de confiance** afin de faire face aux menaces cyber et au contexte géopolitique.

Dans un marché surchargé, il ne suffit plus de gérer des interconnexions fiables mais aussi de disposer d'éléments de protection (filtrage de flux, tunnels VPN, filtrage URL, détection d'intrusions, etc.) pour les différents réseaux. Cela permet d'être en mesure de sécuriser les accès WAN et de protéger les utilisateurs en toutes circonstances. Pour effectuer un choix judicieux, il faut prendre en considération *a minima* les 4 aspects suivants : performance, coût, sécurité et confiance.

Ce livre blanc décrit **les différents aspects qu'une organisation doit considérer dans la mise en place d'une approche Trusted SD-WAN**, en d'autres termes une approche technologique sécurisée et de confiance. Ce document s'adresse aux consultants et responsables sécurité des systèmes d'information pour bien comprendre les enjeux du Trusted SD-WAN à l'heure actuelle.

Implémentation du SD-WAN, pourquoi est-elle indispensable ?

#1

La transformation numérique opérée par les entreprises a modifié les usages des applications qui étaient *on-premise* et utilisées par les collaborateurs connectés depuis les bureaux de l'entreprise. Dans ce cadre, les communications intersites peuvent toujours s'effectuer avec des connexions MPLS[1] pour relier les différentes sites de l'organisation, mais le coût demeure souvent important.

De même, nous identifions l'usage des applications sur le cloud (Microsoft 365, Salesforce etc.) comme un deuxième aspect important.

En effet, cette transformation des entreprises contribue à augmenter les demandes sur les réseaux informatiques étendus (WAN) pour ces deux cas de figure.

Par conséquent, la façon dont les données circulent a évolué et les entreprises se tournent progressivement vers le SD-WAN pour rester compétitives et faire face aux différents challenges technologiques.

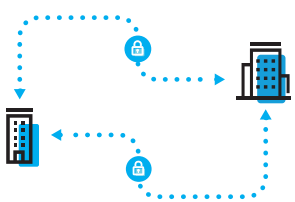
Le SD-WAN est un paradigme d'architecture permettant de **créer un réseau étendu multi-sites et d'assurer la qualité et disponibilité des accès aux applications SaaS[2]/ Web, l'ensemble étant géré depuis un point central**.

1 Créé dans les années 1990, le MultiProtocol Label Switching est un réseau privé qui ne transite pas sur internet. C'est une technologie de moins en moins utilisée.
2 SaaS : Software as a Service. Source

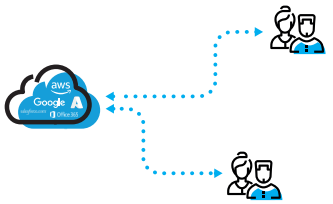
POURQUOI LE SD-WAN EST INDISPENSABLE ?

Cette technologie s'avère être une approche attractive afin d'optimiser les coûts. Comme indiqué dans son nom, il est *Software-Defined* car il permet un contrôle automatique des données grâce à du logiciel afin d'obtenir **des meilleures performances et résilience des applications**.

Il peut gérer le trafic réseau à partir des politiques centralisées selon différents critères comme l'application, l'utilisateur, l'heure, etc. Cela permet d'obtenir un réseau WAN plus rapide et plus fiable.



Communications sécurisées intersites



Connexions de qualité aux applications web
(AWS, Salesforce, Microsoft 365, etc.)

UNE OFFRE ABONDANTE

> *Les entreprises du secteur informatique étendent leurs opérations commerciales à l'échelle mondiale et passent aux plateformes cloud, la demande du marché augmente* ***pour une architecture WAN robuste et sécurisée*** *afin d'obtenir une connectivité élevée et d'améliorer les performances du réseau.*
>
> **— Global Market Insights**

L'évolution des usages a contribué à l'essor du SD-WAN car il permet de mieux gérer les communications intersites et l'accès à des services Web / SaaS. Ce changement des besoins dans le domaine du SD-WAN structure le marché qui s'articule autour de nombreux acteurs.

Entre les acteurs historiques du secteur du réseau, ceux issus de la cybersécurité ou encore les fournisseurs de services Cloud, l'offre est pour le moins pléthorique. Le choix repose ici sur la proposition de valeur entre plusieurs critères : optimisation des liens WAN, simplicité de déploiement, facilité de gestion et de suivi, sécurisation des communications, etc.

Dès lors, **le choix de la solution SD-WAN repose essentiellement sur les cas d'usages à mettre en œuvre**, ainsi que sur l'organisation de l'entreprise et sa sensibilité aux menaces cyber.

Par exemple, une entreprise qui utilise des solutions SaaS pour ses applications métiers critiques aura tendance à choisir un acteur du Cloud. Une organisation multi-sites s'assurera d'un déploiement aisé surtout pour les plus petites agences. Ou encore, une entreprise sensible à la cybersécurité, de par son domaine d'activité ou ses compétences, s'orientera vers un éditeur de solutions de cybersécurité.

La menace cyber
des États-nations

#2

La géopolitique internationale et européenne inclut plus que jamais la cybersécurité comme enjeu stratégique.

En effet, le contexte géopolitique se trouve sous tension et les cyberattaques deviennent de plus en plus organisées, se caractérisant par les éléments suivants[1] : rapidité, évolutivité, réplicabilité et complexité donnant à l'attaquant un avantage structurel. Comme le souligne Philippe Piron, Président de GE Power Conversion & Grid Solutions[2], *« l'attaquant est partout, difficile à détecter et à authentifier, créatif et prompt à développer toujours de nouvelles attaques [...] »*.

Dans ce contexte, les États ne sont pas en reste et s'arment d'outils cyber soit directement soit en s'appuyant sur des groupes organisés.

Comme l'indique le professeur Mike McGuire[3], maître de conférences en criminologie à l'Université de Surrey au Royaume-Uni, les États-nations investissent de plus en plus *« de temps et de ressources à l'obtention d'avantages stratégiques cyber pour promouvoir leurs intérêts nationaux, leurs capacités de collecte de renseignements, et leur puissance militaire par l'espionnage et le vol »*.

1 Philippe Piron in *La cyberdéfense, nouvelle arme géopolitique*. Source
2 *Ibid.*
3 Usine digitale. Source
4 Global Security Mag. Source
5 *Ibid.*

Si ce sont les entreprises à forte valeur ajoutée (industrielles, pharmaceutiques etc.) qui constituent les premières victimes, de façon plus générale, 82%[4] des organisations estiment que géopolitique et cybersécurité sont étroitement liées.

De ce fait, une évaluation fréquente **des risques liés aux attaques par des états-nations devrait constituer un point à considérer dans la stratégie** de protection de chaque organisation. Comme le souligne, Kevin Bocek[5], vice-président en charge de la stratégie de sécurité et des informations sur les menaces chez Venafi : *« chaque organisation doit renforcer les mesures permettant de gérer ses actifs de sécurité cruciaux »*.

Les principales cibles de cyberattaques



Les principales armes cyber utilisées



SD-WAN ET CYBERSÉCURITÉ

Le SD-WAN assure de façon efficace et flexible la disponibilité et la qualité des connexions intersites et aux applications Cloud.

Or, la multiplication de nouveaux usages Web / SaaS entraine une augmentation des risques (dépendance d'Internet, des applications tierces etc.).

Par conséquent, il faut appliquer des couches de sécurité supplémentaires au sein de l'architecture SD-WAN afin de réduire le danger non négligeable en termes d'intrusions et de surveillance de vos communications sensibles.

En synthèse, la connectivité et la criticité des communications WAN au cœur de tous les échanges au sein d'une entreprise requiert une **couche de sécurité et de confiance afin de garantir la confidentialité des données une fois le déploiement du SD-WAN effectué**.

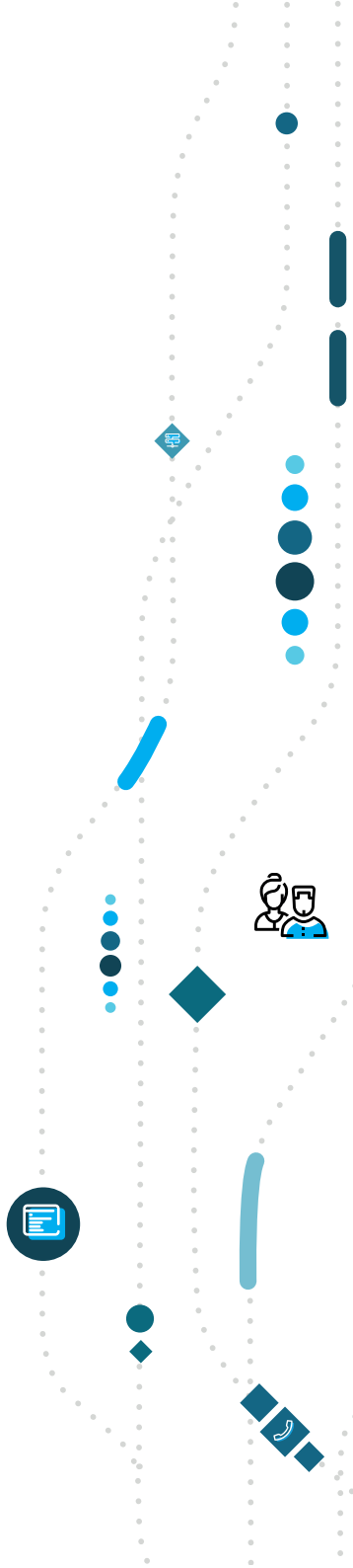
80%

des déploiements de SD-WAN intégreront, dans les prochaines années, des impératifs de services de sécurité d'après Gartner.

Certains acteurs restent réticents à fixer les règles du jeu de la confrontation dans le cyberespace. ***Nous pourrions donc être confrontés à des situations d'escalade rapides et non maîtrisées****, débouchant sur des crises inédites et des effets en cascade non anticipés.*

— Florence Parly
Ministre des armées

Déclaration sur la cybersécurité et la cyberdéfense, Lille le 8 septembre 2021



SD-WAN : **amélioration** de l'expérience applicative

#3

Comme évoqué précédemment, les implémentations de SD-WAN se sont adaptées aux nouveaux usages et à la transformation numérique opérée par les organisations. Comme le signale le cabinet IDC, 70% des applications seront cloud-natives d'ici 2024.

Dans ce contexte, une connexion de qualité doit être présente. Cependant, elle peut être instable (perte de paquets et/ou des retards dans la réception). De ce fait, des questions légitimes peuvent apparaître : comment assurer une qualité stable pour les applications métier critiques ? Quelle qualité vidéo et audio pour les utilisateurs ? Pour combien de sites ?

Le SD-WAN optimise la bande passante afin d'améliorer les performances de celle-ci, selon les différents besoins (VoIP, vidéo, flux d'impression, transfert de fichiers, applications SaaS etc.). Cela permet d'assurer la continuité de service et une expérience optimale à tous les collaborateurs.

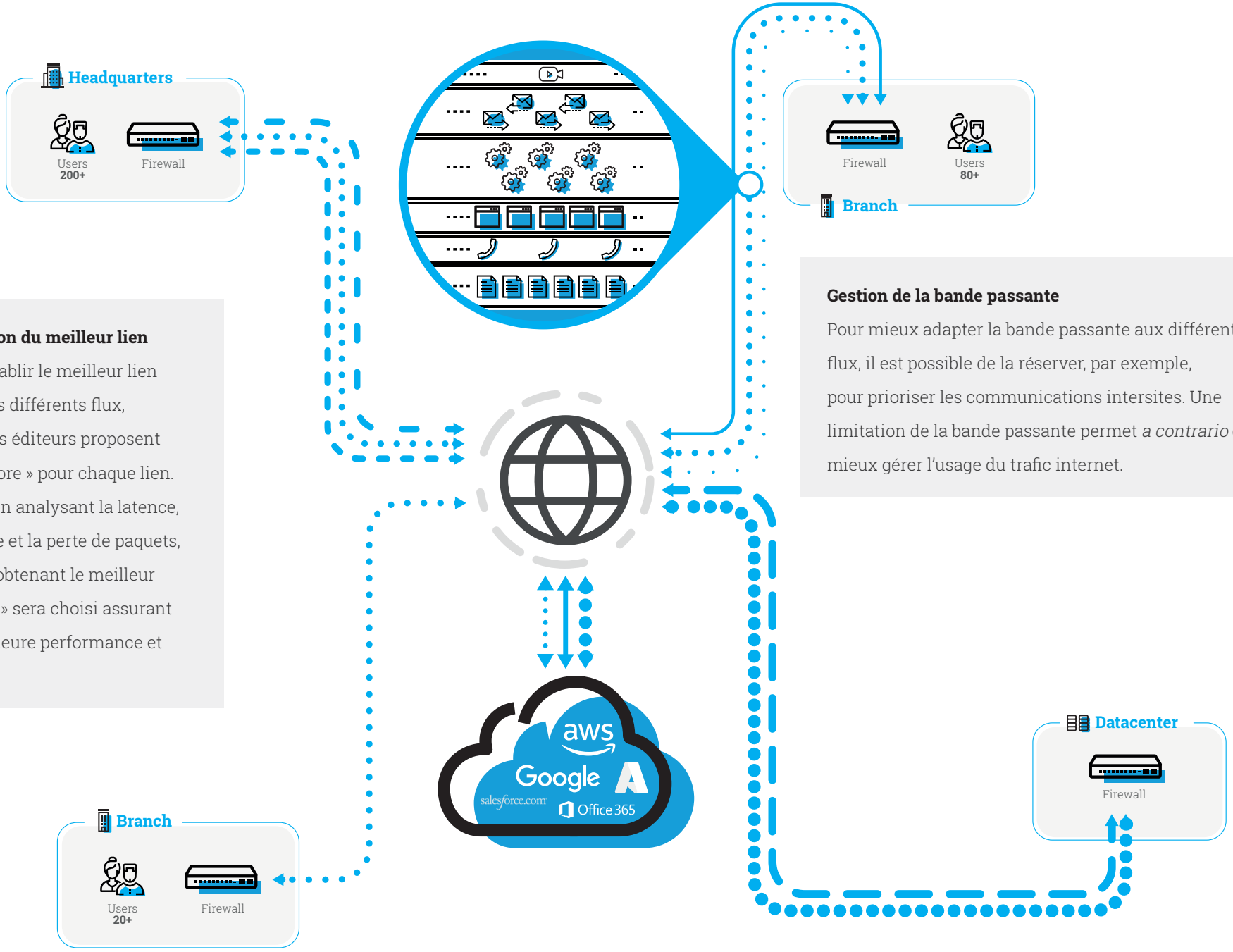
+ de **214** **milliards de dollars** dépensés en services de cloud public en 2019[1]

1 Stéphane Chmielewski in *Pourquoi le SD-WAN est un des piliers de la transformation numérique ?* Source

SÉLECTION DU MEILLEUR LIEN ET GESTION DE LA BANDE PASSANTE

Avec les accès WAN multiples (Internet, succursales etc.) et l'émergence du cloud, **le SD-WAN apporte un vrai avantage avec des débits supérieurs et un ratio économique attractif**, ce qui évite l'investissement dans des liaisons coûteuses. Ainsi, il est possible d'obtenir une connectivité et des performances fiables à tout moment.

Pour gérer au mieux la bande passante et obtenir un niveau de service à la hauteur, il est important de s'orienter vers des solutions qui améliorent les temps de réponse sur les applications et/ou flux utilisés de différents sites pour une meilleure qualité de service.



Sélection du meilleur lien

Pour établir le meilleur lien pour les différents flux, certains éditeurs proposent un « score » pour chaque lien. Ainsi, en analysant la latence, la gigue et la perte de paquets, le lien obtenant le meilleur « score » sera choisi assurant la meilleure performance et qualité.

Gestion de la bande passante

Pour mieux adapter la bande passante aux différentes flux, il est possible de la réserver, par exemple, pour prioriser les communications intersites. Une limitation de la bande passante permet *a contrario* de mieux gérer l'usage du trafic internet.

SD-WAN : **adaptabilité** pour les différents usages

#4

RECONNAISSANCE DES APPLICATIONS

L'approche SD-WAN s'oriente de plus en plus vers une optimisation de l'infrastructure afin de réduire les coûts et d'améliorer l'accès aux applications fournies en cloud.

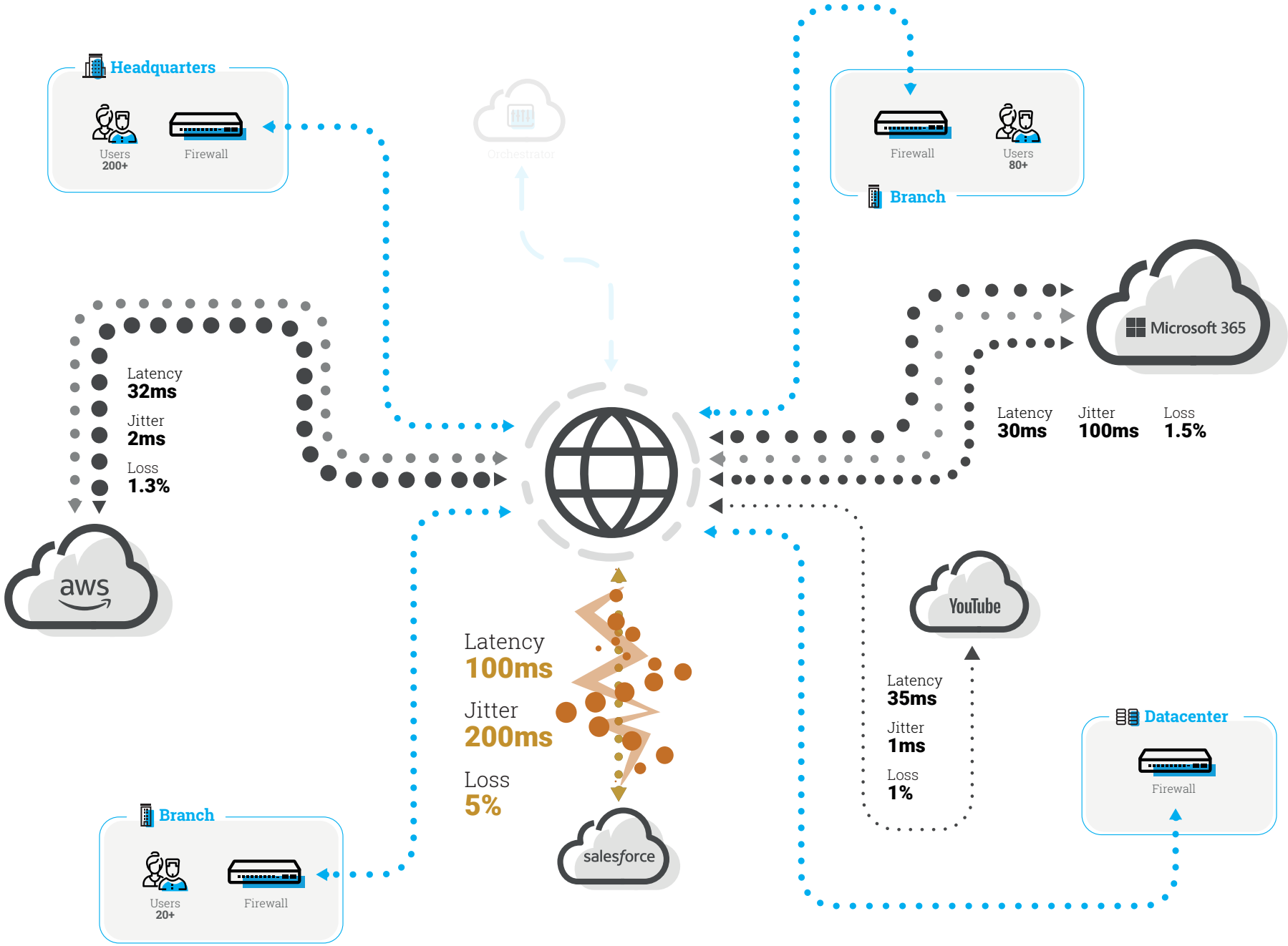
Cette transformation des architectures SD-WAN s'articulent autour du maintien de la qualité expérience utilisateur. De ce fait, la plupart des éditeurs optent aujourd'hui pour une reconnaissance approfondie des données transitant dans les flux (par exemple, HTTPS).

Cela permet de mieux distinguer les différentes applications cloud (standards ou personnalisées). **Cette identification améliore la visibilité et assure une définition des politiques de qualité de service (QoS) et de *service level agreement* (SLA) spécifiques en adéquation à chaque application**.

Ces solutions garantissent ainsi de hautes performances pour les différentes applications SaaS utilisées (Zoom, AWS, Salesforce, Google...) tout comme celles en relation directe avec les clients.

Pour aller plus loin dans l'analyse du trafic réseau, il ne faut pas oublier que la composante sécurité doit être présente pour assurer une bonne protection des échanges.

Cela se traduit par un filtrage web exhaustif et en temps réel du trafic, une analyse de type DPI IPS afin d'éliminer tout risque de non-conformité des paquets transitant par l'infrastructure ou encore une inspection SSL des différents protocoles web afin de garantir un usage conforme à la politique de sécurité établie.


Headquarters
Users
200+
Firewall
Orchestrator
Firewall
Users
80+
Branch
Microsoft 365
Latency
30ms
Jitter
100ms
Loss
1.5%
Latency
32ms
Jitter
2ms
Loss
1.3%
aws
Latency
100ms
Jitter
200ms
Loss
5%
salesforce
YouTube
Latency
35ms
Jitter
1ms
Loss
1%
Datacenter
Firewall
Branch
Users
20+
Firewall

La **nécessaire sécurisation** des communications

#5

COMMUNICATIONS SÉCURISÉES

La garantie de la confidentialité et intégrité des données, liée à la criticité des communications WAN au sein d'une entreprise repose sur la sécurisation des communications intersites. **Les données critiques se doivent d'être chiffrées afin de s'assurer qu'elles restent inexploitables par toute personne n'ayant pas le droit d'y accéder**.

Élement essentiel des réseaux étendus depuis plusieurs années, le VPN IPsec est un protocole disposant d'un ensemble de normes qui permet de connecter de manière sécurisée les différents sites sur un WAN via Internet. Cette méthode d'interconnexion peut être utilisée pour tous les usages, vers toutes les destinations avec un coût presque nul.

Ainsi, **le réseau SD-WAN doit proposer un chiffrement robuste et de bout-en-bout.** De ce fait, la sécurisation des données transitant entre les différents sites d'une entreprise doit passer par la mise en place de tunnels VPN IPsec.

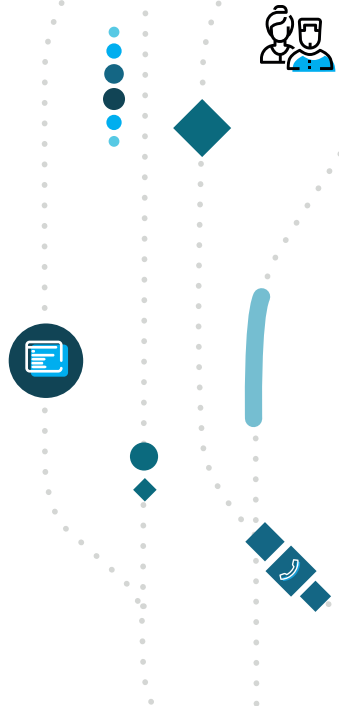


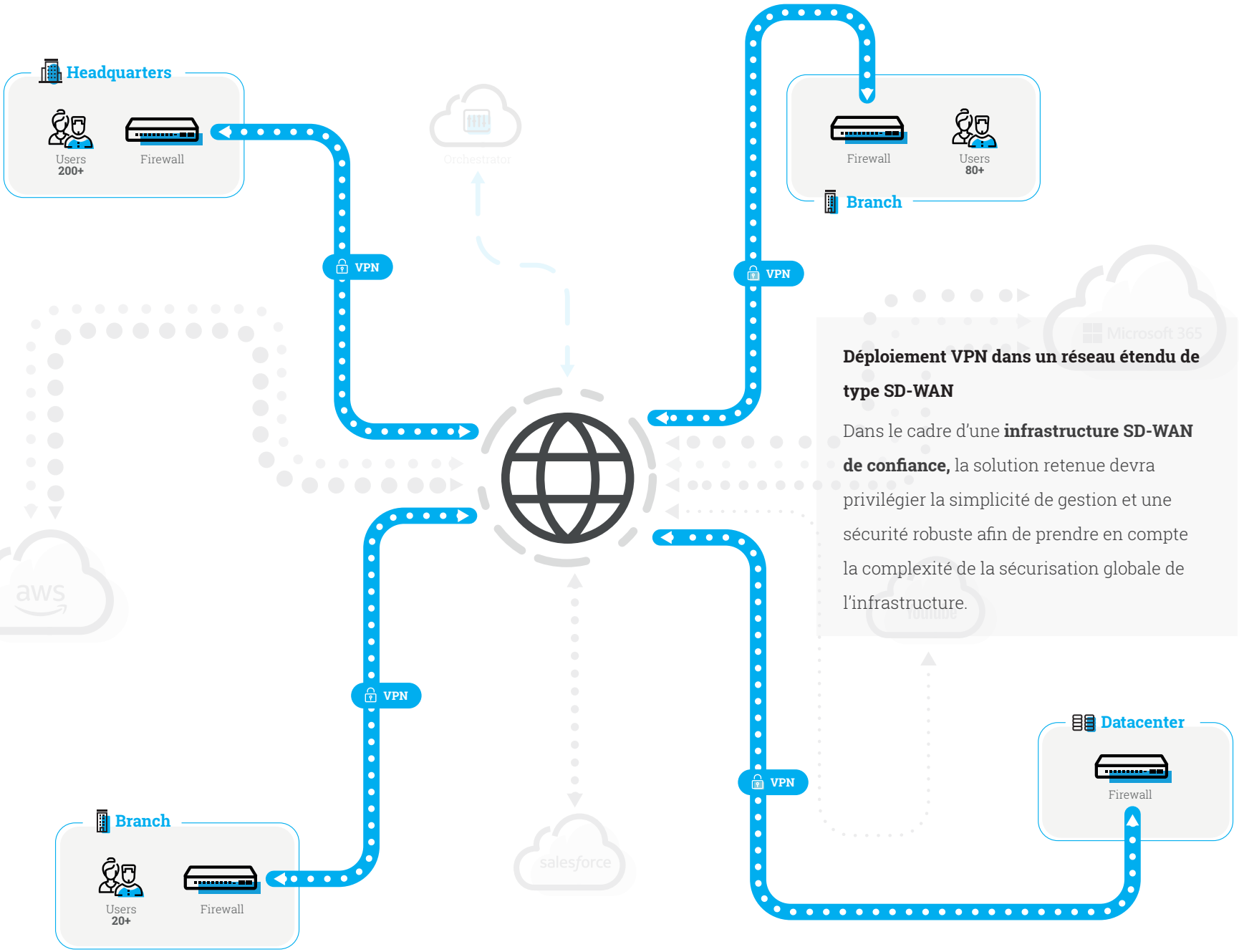
Le saviez-vous ?

Afin de renforcer le niveau de sécurité de manière efficace, le VPN IPsec peut être utilisé comme une mesure de sécurité complémentaire pour « encapsuler des protocoles qui sont déjà sécurisés par d'autres mécanismes[1] ».

Guide ANSSI-NT_ IPsec Source







Déploiement VPN dans un réseau étendu de type SD-WAN

Dans le cadre d'une **infrastructure SD-WAN de confiance,** la solution retenue devra privilégier la simplicité de gestion et une sécurité robuste afin de prendre en compte la complexité de la sécurisation globale de l'infrastructure.

Gestion efficace du SD-WAN

#6

L'implémentation d'une architecture SD-WAN qui s'appuie sur une gestion centralisée facilite le déploiement et les mises à jour de l'infrastructure tout en offrant une visibilité globale.

Ainsi, depuis une unique console d'administration, il est possible de déployer ou de modifier les fonctions de sécurité et les politiques de routage sur plusieurs sites au lieu d'envoyer un technicien sur place.

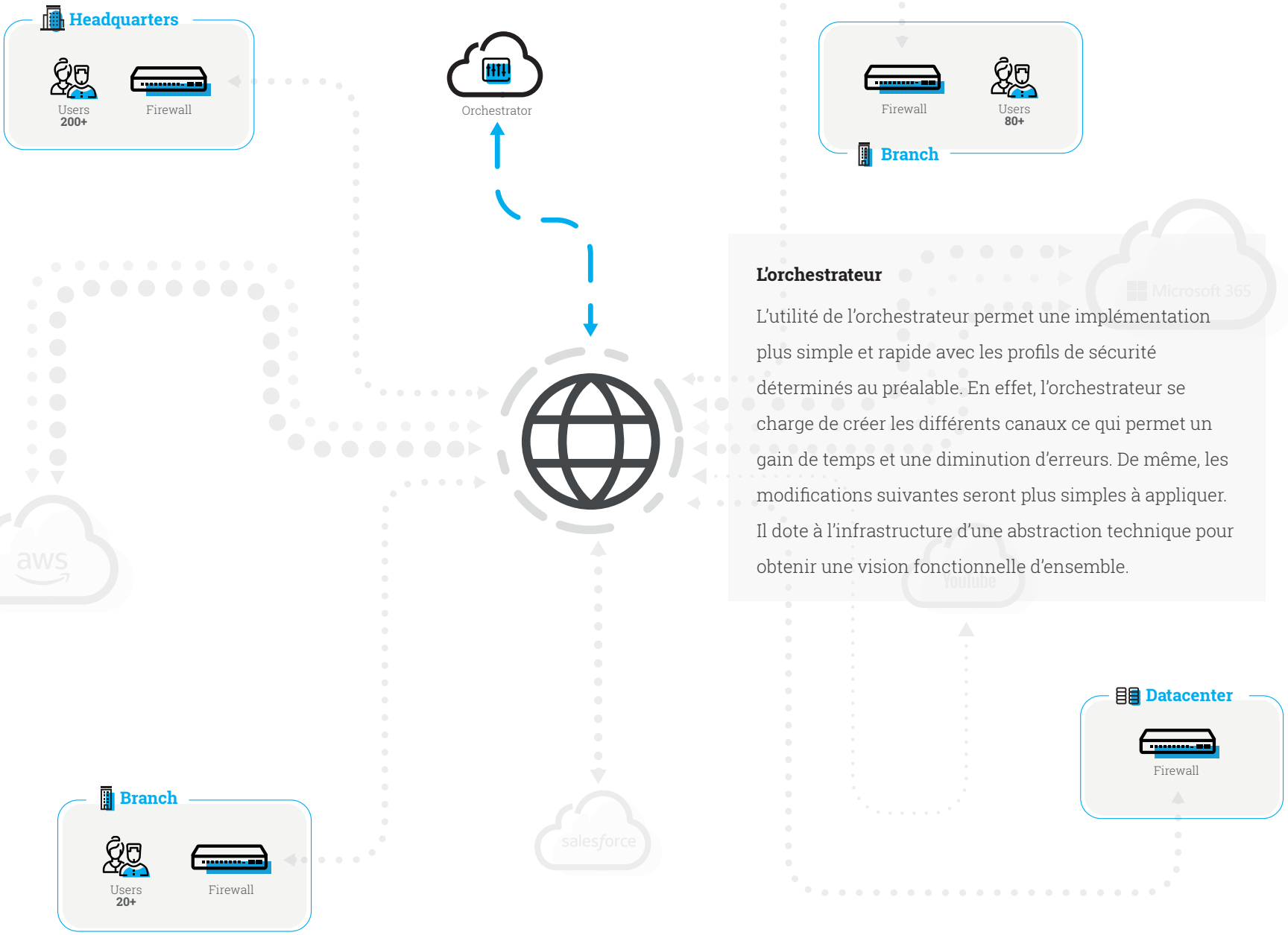
En quelques clics, il est aussi possible de définir les différentes interactions entre les sites puis l'orchestrateur se charge de configurer l'ensemble des équipements de connexions et de sécurité.

ORCHESTRATION

D'autre part, la visibilité globale apportée par les solutions d'orchestration assure **une vision à 360°sur l'état de l'infrastructure et des performances de chaque application**. Cette surveillance offre également la possibilité de remonter des indicateurs de SLA (latence, gigue, perte des paquets) sur la qualité des liens.

Cette vision globale permet ainsi de mettre en place une politique de gestion efficace de bande passante (QoS) afin de garantir une connectivité fiable à tout moment. Enfin, cette vision globale apporte avantageusement une visibilité sur le shadow IT.

En synthèse, la solution d'orchestration choisie doit **apporter la nécessaire couche de confiance dans la sécurité du réseau tout en permettant de simplifier sa configuration**. Ses fonctions de supervision assurent un suivi des indicateurs de qualité de liens tout en permettant la gestion d'événements (logs) et d'incidents de sécurité.



L'orchestrateur

L'utilité de l'orchestrateur permet une implémentation plus simple et rapide avec les profils de sécurité déterminés au préalable. En effet, l'orchestrateur se charge de créer les différents canaux ce qui permet un gain de temps et une diminution d'erreurs. De même, les modifications suivantes seront plus simples à appliquer. Il dote à l'infrastructure d'une abstraction technique pour obtenir une vision fonctionnelle d'ensemble.

Trusted SD-WAN : **le choix de confiance**

#7

TRUSTED SD-WAN

Comme indiqué au préalable, le SD-WAN optimise les communications distantes et les accès au Cloud mais la sécurisation doit également faire partie de l'équation. À cet effet, une question légitime se pose : existe-t-il des architectures SD-WAN sécurisées certifiées et/ou homologuées par un organisme de certification indépendant ?

En l'état actuel, nous constatons qu'il n'existe pas de certifications ou de qualifications SD-WAN indépendantes des fournisseurs prônant cette approche technologique.

Par conséquent, il est important de disposer d'éléments concrets pour juger objectivement la solution SD-WAN choisie. À l'heure de sélectionner un éditeur parmi plusieurs solutions matérielles et logicielles, il faut se questionner, entre autres, sur la robustesse du produit et la confiance au regard des enjeux géopolitiques et économiques.

D'un côté, comme le souligne l'ANSSI[1], la **robustesse** « *consiste à éprouver leur capacité à résister à des attaques informatiques selon un contexte d'emploi et un niveau de menace définis* ».

Ainsi, il faut privilégier des solutions qui prennent en considération ce point pour la sécurisation globale de l'infrastructure SD-WAN.

D'un autre côté, il est important de retrouver la notion de **confiance** de façon claire dans la stratégie produit afin de respecter les engagements pris auprès d'un organisme de certification / qualification officiel.

En synthèse, compte tenu de l'absence d'homologation officielle de SD-WAN, il faut s'appuyer sur les différentes certifications / qualifications produit ainsi que les différentes référentiels de sécurité fournis par les autorités gouvernementales afin de disposer d'une architecture de type Trusted SD-WAN.

Le savez-vous ?

Le durcissement ou hardening est le processus visant à sécuriser un système.

Cette démarche consiste à **réduire à l'indispensable les composants logiciels installés sur le système, les outils, les utilisateurs et les droits non indispensables** tout en disposant des fonctionnalités nécessaires au bon fonctionnement.

1 ANSSI, Source

ASSURER UNE QUALITÉ LOGICIELLE

Les connexions des sites distants et les accès au cloud via le SD-WAN augmentent la connectivité mais ils peuvent également augmenter les risques de sécurité si cette composante n'est pas prise en compte.

En effet, les solutions qui constituent le SD-WAN, représentent une cible d'attaque pour les cyber-criminels. D'ailleurs, comme le souligne l'ANSSI[1], les éléments logiciels d'une infrastructure se doivent être vérifiés et leur configuration durcie avant leur exploitation.

Également, comme évoqué précédemment, il faut **privilégier des éditeurs de confiance qui sont en mesure de proposer des produits soit qualifiés soit certifiés** par des organismes tiers et légitimes comme l'ANSSI en France, le CCN en Espagne, le BSI en Allemagne ou encore l'ENISA au niveau européen. Effectivement, ils garantissent la conformité vis-à-vis des exigences réglementaires, techniques et de sécurité.

Cela assure une protection robuste du produit et comme l'indique l'ANSSI [...] « *d'engagement du fournisseur de solutions à respecter des critères de confiance* »[2]. En outre, pour atteindre un niveau de robustesse élevé, les produits doivent éprouver une résistance aux cyberattaques selon un cadre spécifique. Cela passe, entre autres, par un audit du code source du produit en question.

Comme nous venons de le voir, il n'existe pas aujourd'hui sur le marché des solutions SD-WAN certifiées et/ou qualifiées. Pour pallier ce manque, il faut en amont analyser les éléments indépendamment afin de choisir un ou plusieurs fournisseurs proposant des produits robustes et de confiance (qualifiés de préférence), avec des fonctionnalités SD-WAN (orchestration, optimisation de la QoS...) et des options de sécurité (pare-feux, filtrage de flux, VPNs...) afin d'obtenir un ensemble efficace protégeant votre infrastructure à tout moment.

VPN IPsec

DR

Sécurisation des interconnexions

« Les interconnexions de SI DR doivent être sécurisées au moyen de tunnels VPN garantissant la protection de tous les flux échangés (confidentialité, intégrité, antirejeu, authentification mutuelle des extrémités) ». Dans ce but, l'organisation a défini un protocole VPN IPsec DR.

ANSSI, Guide ANSSI-PG-075 Source

1 ANSSI dans *Guide de recommandations pour les architectures et systèmes d'informations sensibles.* Source
2 ANSSI. Source

Les 4 points essentiels **pour choisir votre Trusted SD-WAN**

#1

Privilégiez un fournisseur reconnu par un organisme officiel et indépendant (ANSSI, CCN etc.)

#2

Assurez-vous que l'éditeur dispose des éléments SD-WAN et de sécurité pour une meilleure couverture fonctionnelle. Une architecture tout-en-un sécurisée : usage d'une appliance pour unifier entre autres le SD-WAN, le pare-feu et les connexions sécurisées de bout en bout.

#3

Favorisez des technologies disposant d'une visibilité unifiée. Optimisation dans la gestion et meilleure centralisation des différentes fonctions.

#4

Disposez d'une gestion efficace des applications cloud (Microsoft 365, Salesforce etc.)

Trusted SD-WAN by Stormshield : **confiance et sécurité tout-en-un**

#8

Stormshield vous accompagne **pour une intégration du Trusted SD-WAN** dans votre infrastructure **de façon sécurisée et performante**



Gérez aisément votre réseau étendu

Grâce aux fonctionnalités SD-WAN de Stormshield, **centralisez et maîtrisez vos connexions intersites et les accès au Cloud** de votre infrastructure étendue.



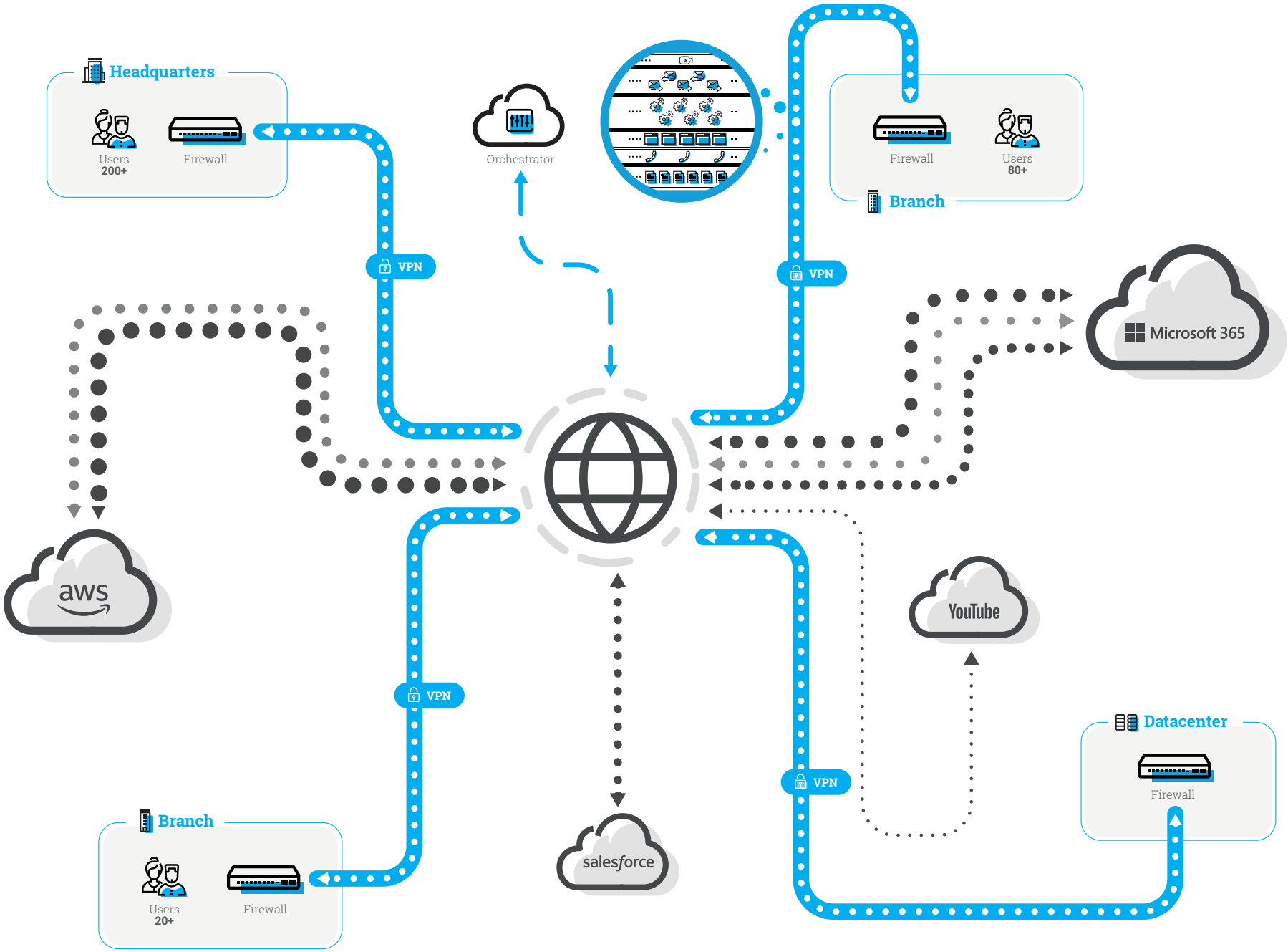
Sécurisez votre SD-WAN à tout moment

Ayez l'esprit tranquille car Stormshield vous propose une technologie SD-WAN sécurisée **pour une protection inégalée de toutes vos connexions**. Vos collaborateurs disposent d'un accès sécurisé aux ressources de l'entreprise où qu'ils se trouvent et depuis n'importe quel terminal.



Choisissez votre SD-WAN de confiance

Basé sur une technologie certifiée au plus haut niveau européen, le SD-WAN de Stormshield vous apporte toute la confiance pour cyber-séréniser votre infrastructure.


Headquarters
Users
200+
Firewall
Orchestrator
Firewall
Users
80+
Branch
VPN
VPN
Microsoft 365
aws
VPN
YouTube
Datacenter
Firewall
VPN
salesforce
Branch
Users
20+
Firewall

LE **CHOIX EUROPÉEN** DE LA **CYBERSÉCURITÉ**

www.stormshield.com

Toute diffusion, reproduction ou représentation, même partielle de ce livre blanc, à d'autres fins qu'une utilisation privative sur un quelconque support, est interdite et pourrait engager la responsabilité civile et pénale de la personne qui ne respecterait pas cette interdiction.

Copyright © 2022 Stormshield