SOPHOS

Évoluer vers le SD-WAN avec Sophos : 6 scénarios d'utilisation

Introduction

Les entreprises distribuées sont de plus en plus répandues dans le monde connecté d'aujourd'hui. La capacité à relier des sites très dispersés géographiquement pour échanger des informations et fournir des applications a changé la manière dont les entreprises fonctionnent, dont les écoles assurent l'éducation des élèves et dont les hôpitaux soignent les patients.

Quel que soit la taille ou le secteur industriel, les entreprises distribuées ont en commun un certain nombre de besoins. Il s'agit par exemple de pouvoir partager des données, de mettre à disposition des applications Cloud et SaaS ou de faciliter les communications et les transactions entre les bureaux distants et les sièges sociaux. Protéger chacun des sites contre les cyber menaces (ransomwares, malwares, piratages, etc.) est aujourd'hui crucial. Les entreprises distribuées veulent également avoir la souplesse nécessaire pour créer de nouveaux sites et ajouter rapidement de nouvelles applications et de nouveaux services. La gestion d'une telle infrastructure peut se révéler très chronophage et les coûts peuvent rapidement s'additionner avec le temps, c'est pourquoi il est important d'avoir les outils d'orchestration nécessaires.

Traditionnellement, de nombreuses entreprises utilisent le protocole MPLS (Multi-Protocol Label Switching), une technique de routage apparue il y a une vingtaine d'années. Le MPLS offre des avantages qui vont au-delà de la simple connexion de sites géographiquement distribués. Par exemple, en dirigeant les paquets d'un nœud de réseau vers un autre en fonction du chemin le plus court disponible, le MPLS fournit une haute qualité de service pour les applications en temps réel sensibles à la latence, telles que la voix et la vidéo. Le MPLS présente cependant des inconvénients. En effet, avec l'adoption du Cloud Computing, les services assurant le réacheminement du trafic à travers un centre de données ne sont plus la meilleure solution. Sans compter que le MPLS n'est pas disponible partout. Mais la principale raison pour laquelle les entreprises distribuées s'éloignent du MPLS est son coût. L'émergence de technologies alternatives, telles que les réseaux étendus à définition logicielle ou SD-WAN (Software-Defined Wide Area Network), permet aux entreprises de créer rapidement de nouveaux sites, de connecter ces sites, d'échanger des informations et de distribuer des applications à un coût nettement inférieur à celui du MPLS.

Le SD-WAN est essentiellement une technique de liens qui s'ajoutent à l'architecture WAN existante. Il peut exploiter n'importe quel service de transport, y compris DSL, câble, 3G/4G/LTE et même MPLS, pour diriger intelligemment le trafic sur le WAN, de la source à la destination, avec un minimum ou aucune latence, gigue ou perte de paquets. L'objectif est d'offrir une expérience utilisateur exceptionnelle grâce à une qualité de service élevée. Et l'amélioration de la qualité de service, à son tour, stimule les gains de productivité. Les entreprises disposent de plusieurs options pour déployer le SD-WAN. Les fournisseurs spécialisés dans le SD-WAN offrent davantage de solutions riches en fonctionnalités, mais le coût de l'appareil, combiné à la gestion continue et à l'absence de sécurité intégrée, peut s'avérer prohibitif. C'est pourquoi un grand nombre d'entreprises sont désormais à la recherche de capacités SD-WAN intégrées dans leur pare-feu.

L'évolution vers le SD-WAN

Le SD-WAN continue de gagner en popularité. Selon Gartner, le taux de croissance annuel composé (TCAC) pourrait atteindre 59 % d'ici 2021, pour devenir un marché de 1,3 milliard de dollars. Le SD-WAN apporte aux entreprises distribuées des avantages significatifs à moindre coût, ce qui explique une transition plus aisée et abordable vers la technologie. Voici les principales raisons expliquant cette projection.

Réduction des dépenses : Bien que le MPLS puisse encore justifier son utilisation dans votre réseau pour répondre à certains besoins, évoluer une partie ou la totalité de vos connexions vers le SD-WAN vous aidera à faire des économies. Ce dernier profite de services Internet et à large bande accessibles au public et moins chers, ce qui vous permet de réduire considérablement vos coûts d'exploitation. Et, si vous cherchez à mettre à niveau votre périphérique WAN, vous pouvez réduire votre investissement en achetant un périphérique qui intègre la technologie SD-WAN.

Performances constantes et prévisibles des applications : Les applications lentes peuvent tirer les entreprises vers le bas. Le SD-WAN vous permet d'utiliser plusieurs connexions haut débit fournies par un seul ou plusieurs fournisseurs d'accès à Internet (FAI). Par cette méthode, les performances des applications sur le WAN sont toujours rapides et disponibles, et cela vous permet de dépenser moins d'argent que si vous utilisiez un MPLS. Vous pouvez également limiter les applications non critiques et acheminer le trafic plus rapidement vers celles qui sont plus importantes pour vous.

Plus de flexibilité : Lorsque vous vous abonnez à un service MPLS, vous êtes « lié » à un seul fournisseur pour toute la durée du contrat. Avec le SD-WAN, vous avez au contraire la possibilité d'ajouter et de supprimer des FAI tout en profitant de fournisseurs locaux offrant des tarifs encore plus avantageux. Vous pouvez également continuer d'utiliser le MPLS entre le siège social et les sites plus importants, et connecter les bureaux plus petits à l'aide du SD-WAN.

Meilleure agilité : Les entreprises en croissance ont besoin d'ajouter rapidement de nouveaux sites et de nouvelles applications pour répondre à l'augmentation de la demande. Parce qu'il s'agit d'une superposition, ou d'un réseau virtuel, le SD-WAN vous permet d'évoluer rapidement et d'accélérer le déploiement de sites supplémentaires. Vous pouvez également ajouter de la bande passante pendant les périodes de forte utilisation d'Internet, mais aussi pour accommoder les nouveaux sites.

Sophos SD-WAN peut vous aider

Quels que soient le type ou la taille de votre entreprise, Sophos peut vous aider à construire un réseau distribué sécurisé qui utilise la technologie de SD-WAN pour connecter votre site central avec vos sites distants et vos succursales. Avec Sophos, vous diminuerez vos dépenses et votre coût global de possession (TCO) en remplaçant le protocole MPLS par des services Internet peu coûteux, tout en vous débarrassant du matériel inutile. Nous avons intégré le SD-WAN dans XG Firewall, y compris les options matérielles, logicielles et appliances virtuelles. Vous pouvez maintenant obtenir tous les avantages d'un éditeur de sécurité de pointe pour protéger la transmission des données confidentielles, tout en maintenant des performances constantes et la disponibilité des applications Cloud (Office 365, Salesforce, G Suite, Microsoft Azure, etc.) sur l'ensemble de votre réseau global et local.

Avantages de Sophos XG Firewall avec SD-WAN

XG Firewall doté de la dernière version du firmware bénéficie des nombreux avantages du SD-WAN.

Réduction des coûts : Avec l'intégration du SD-WAN dans chaque pare-feu Sophos XG, vous n'avez pas besoin d'une solution SD-WAN autonome. Remplacer une partie ou la totalité des connexions réseau MPLS par des services Internet moins onéreux vous permettra aussi de réduise vos dépenses.

Optimisation de la protection : Les pare-feu Next-Gen de la série XG sont disponibles sous format matériel, logiciel, virtuel et Cloud. Ils offrent une protection maximale contre les malwares, les ransomwares, les intrusions et toutes autres menaces sur l'ensemble de votre réseau distribué.

Architecture Xstream : XG Firewall apporte une nouvelle approche dans la manière d'identifier les risques cachés, de se protéger contre les menaces et de répondre aux incidents sans nuire aux performances. Notre architecture Xstream pour XG Firewall utilise une architecture unique de traitement des paquets qui offre des niveaux extrêmes de visibilité, de protection et de performance.

Déploiement Branch-in-a-Box : Créez et déployez votre propre solution SD-Branch dans chaque site distant avec nos périphériques RED Edges uniques et abordables ou nos périphériques de bureau modulaires XG Firewall. Ils intègrent le SD-WAN, des fonctionnalités robustes de gestion du réseau et de la sécurité, en plus d'options LTE et sans fil haute vitesse dans un seul appareil administré de manière centralisée.

Maintien de la continuité des activités : Maintenez votre organisation opérationnelle grâce à des connexions redondantes fournies par les mêmes — ou différents — FAI pour gérer le routage, le basculement et la préservation des sessions en cas de défaillance potentielle du WAN ou de panne.

Choix de RED : Réduisez davantage vos coûts avec les périphériques Sophos SD-RED (Remote Ethernet Devices) bon marché. Les périphériques SD-RED transmettent le trafic chiffré du site distant vers un pare-feu local ou central qui scanne les données à la recherche de menaces avant de les envoyer sur Internet.

Synchronisation : Le système unique de Sécurité synchronisée de Sophos partage en temps réel des informations entre les produits Sophos sur le réseau distribué via notre technologie Security Heartbeat™. Vous obtenez ainsi la réponse automatisée aux incidents de sécurité.

Optimisation des performances des applications : Contrairement au MPLS, qui pénalise les performances en réacheminant le trafic du site distant vers le centre de données de l'entreprise puis vers Internet, le SD-WAN élimine les goulots d'étranglement et la latence en se connectant directement à Internet pour un accès plus rapide aux applications Cloud.

Plus d'agilité : Déployez rapidement des sites distants sans l'intervention d'un informaticien sur site grâce au déploiement Zero-Touch de Sophos. Ajoutez et distribuez de nouveaux services et applications Cloud rapidement sur l'ensemble de votre infrastructure de réseau.

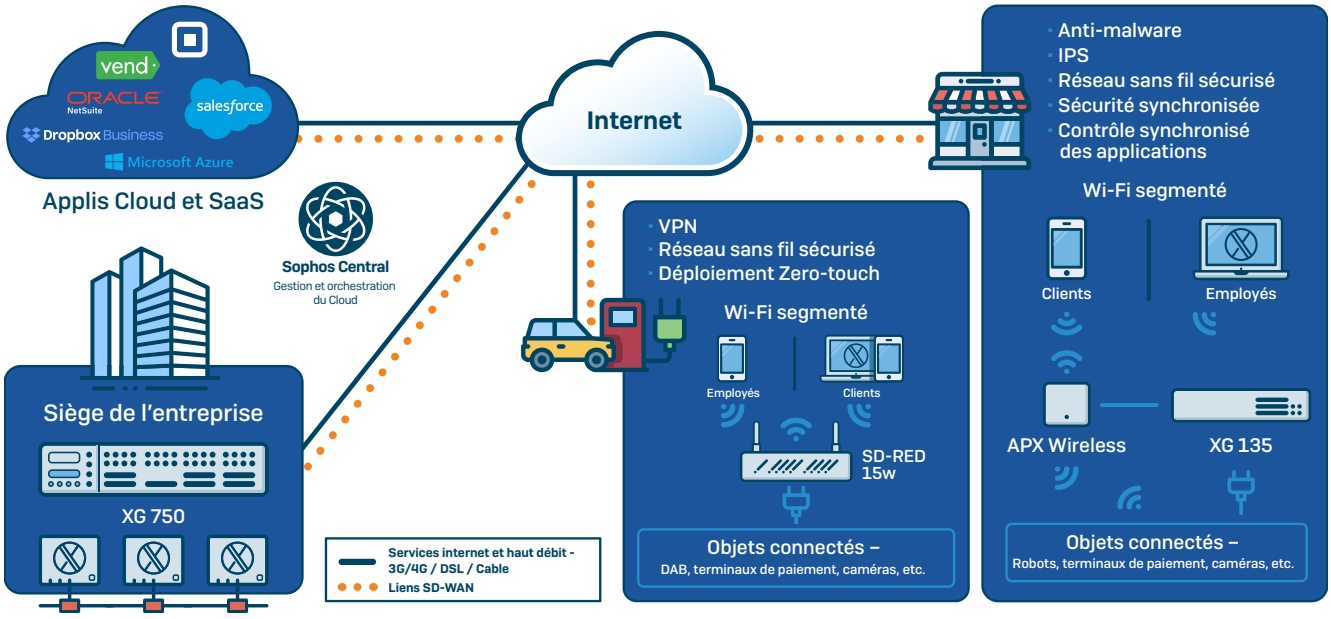
Amélioration de la visibilité et du contrôle des applications : Obtenez une visibilité sans précédent sur l'utilisation des applications sur votre réseau. Le SD-WAN synchronisé est une fonctionnalité de la sécurité synchronisée de Sophos. Il exploite le contrôle synchronisé des applications de Sophos pour identifier de manière plus précise et plus fiable les applications. Cela permet d'identifier 100 % des applications inconnues, évasives et personnalisées afin que vous puissiez facilement prioriser les applications souhaitées et bloquer celles non souhaitées. Ajoutez ces applications précédemment non identifiées aux politiques de routage SD-WAN pour un niveau de contrôle et de fiabilité qu'aucun autre pare-feu ne peut égaler.

Orchestration : Coordonnez et automatisez les fonctions réseau plus efficacement avec des API puissantes. Puis administrez l'intégralité de votre réseau distribué en tous lieux dans Sophos Central, la plateforme de gestion unifiée de Sophos basée dans le Cloud.

Scénarios d'utilisation de Sophos SD WAN

Déployez Sophos XG Firewall et SD-RED dans les scénarios d'utilisation suivants pour connecter de manière sécurisée des sites distants et des succursales avec un site central.

1. Commerce de détail



Description : Les chaines de distribution sont formées par de multiples magasins ou franchises qui échangent des données financières et personnelles sur leurs clients par le biais de transactions en ligne ou en magasin.

a. Connectez les magasins franchisés et les appareils connectés à Internet à l'intérieur ou à l'extérieur du bâtiment, y compris les terminaux de paiement (POS), kiosques, signalisation numérique et objets connectés.

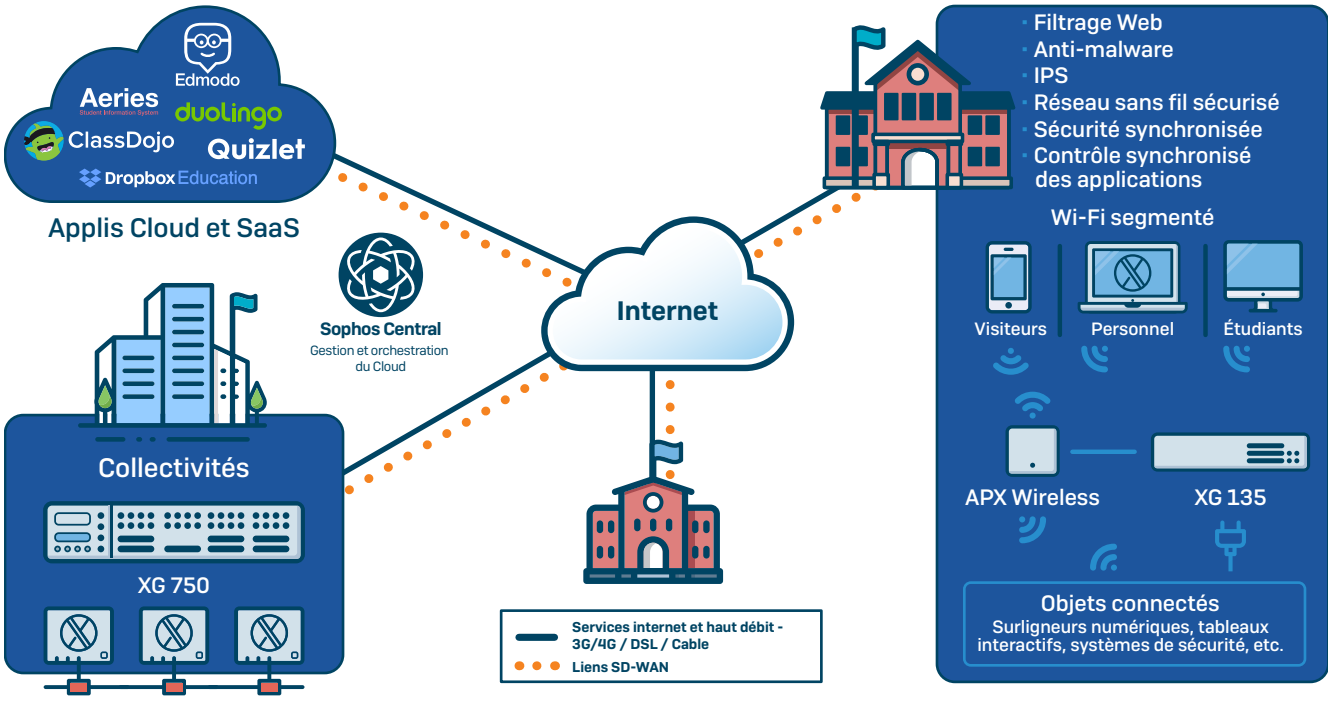
b. Sécurisez la transmission des données confidentielles des clients vers le site central par les terminaux de paiement.

c. Suivez l'évolution des nouvelles technologies des terminaux de paiement, comme les paiements par appareil mobile et les coupons électroniques.

d. Fournissez à vos clients un accès à Internet via un réseau Wi-Fi isolé de celui utilisé par les employés.

e. Conformez-vous aux réglementations PCI DSS (États-Unis) et RGPD (UE).

2. Secteur de l'éducation



Description : Des écoles primaires et secondaires regroupées à l'échelle des collectivités pour assurer l'éducation des élèves.

a. Connectez les écoles et les collectivités.

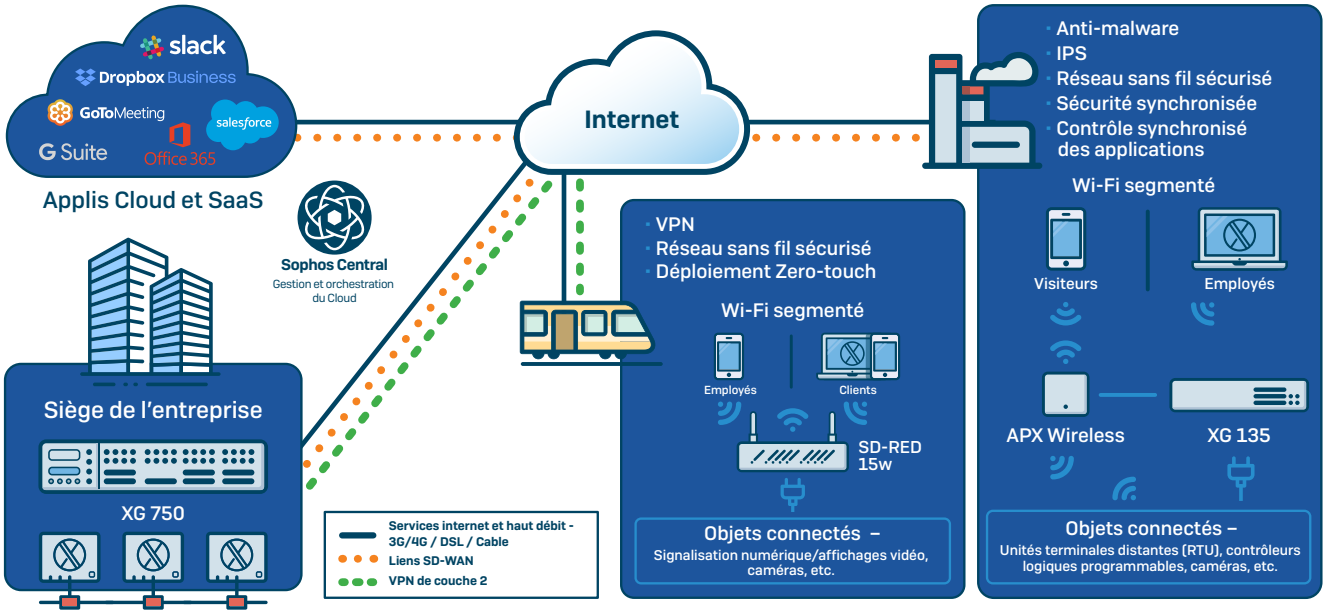
b. Échangez de manière sécurisée des informations confidentielles sur les étudiants et le personnel enseignant, et des transactions financières.

c. Gérer le nombre croissant de nouveaux appareils qui accèdent au réseau, qu'ils soient personnels ou en lien avec l'établissement scolaire.

d. Suivez le rythme de la hausse des technologies et des applications éducatives sur le réseau.

e. Conformez-vous aux exigences réglementaires de la CIPA (États-Unis).

3. Systèmes de commande industriels, dispositifs à distance et véhicules



Description : Les entreprises de production, de services publics, de transport, de construction, etc., qui utilisent des technologies ICS (partage de connexion Internet) (par ex. systèmes SCADA), des dispositifs à distance (par ex. caméras de surveillance) ou des transports publics (par ex. métro) pour soutenir les infrastructures cruciales.

a. Connectez à la fois les sites statiques (usines, terminaux, gares, centrales) et les véhicules (bus, trains, avions) qui voyagent continuellement entre votre bureau central et les lieux de destination.

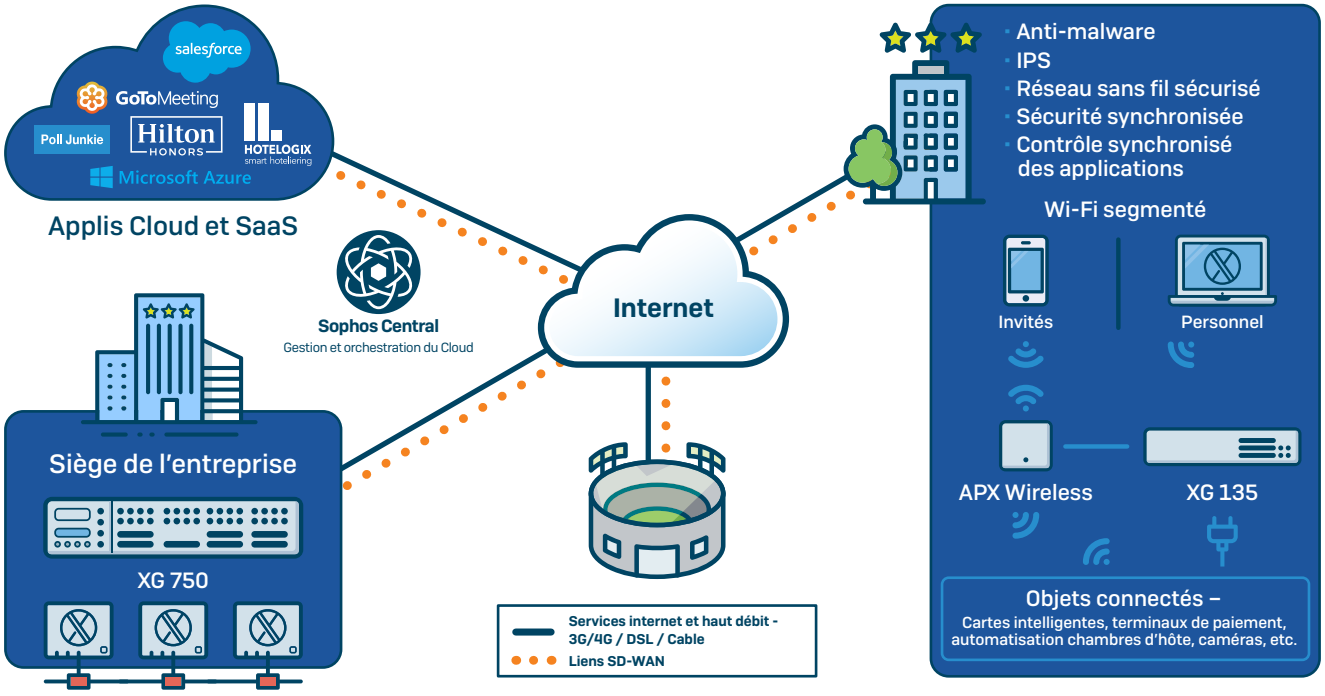
b. Protégez les données recueillies par les capteurs et les instruments mobiles des sites distants qui sont retransmises vers un hôte central.

c. Suivez le rythme de l'évolution des technologies des terminaux de paiement et des objets connectés sur le réseau.

d. Protégez les transactions financières et fournissez aux clients un accès à Internet et au streaming (par ex. films et musique).

e. Déployez des périphériques Sophos SD-RED sur chaque site et sur chaque véhicule pour profiter d'une solution de connectivité SD-WAN abordable et Zero-Touch.

4. Hôtellerie et accueil



Description : Les chaines hôtelières régionales et internationales et les sociétés de gestion de structures d'accueil et d'événements qui offrent des services d'hébergement et de divertissement.

a. Connectez les propriétés hôtelières et/ou les lieux d'accueil et d'événements pour partager des informations confidentielles sur les clients et assurer des services entre chaque lieu et le siège social de la société.

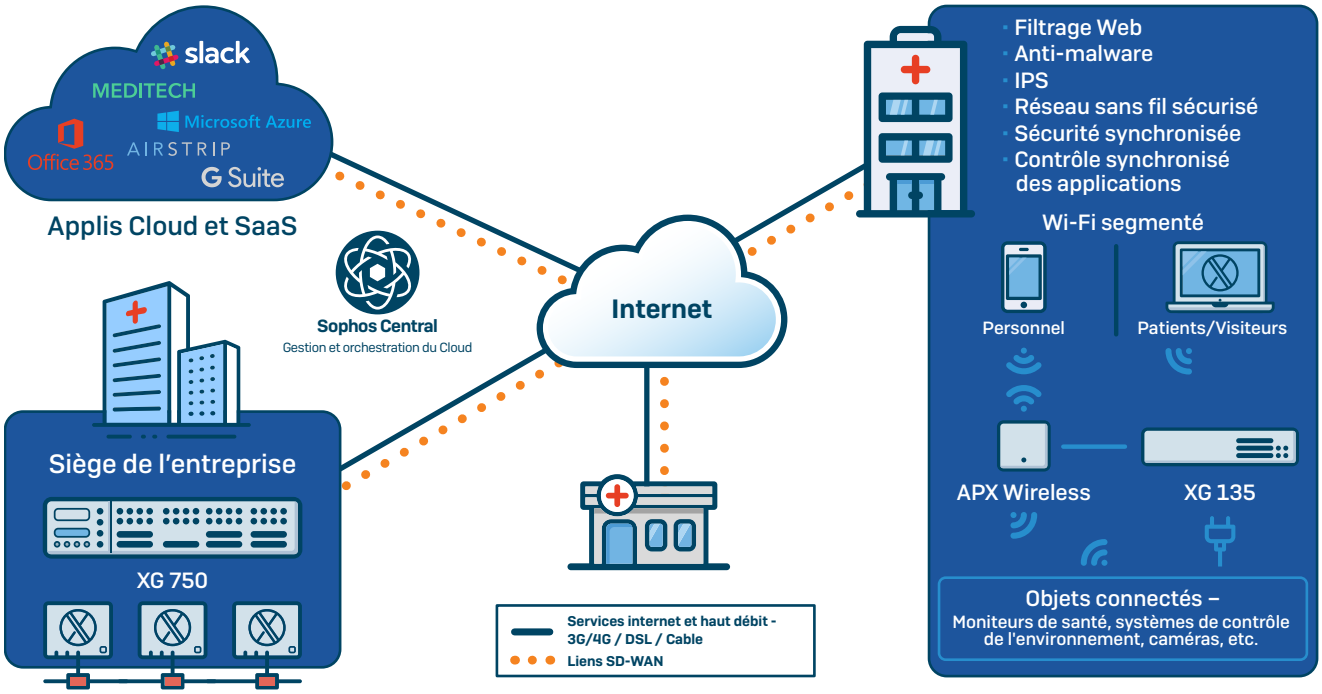
b. Fournissez aux invités et aux clients des services tels qu'un accès au réseau Wi-Fi, des clés numériques, du contenu en streaming et un système de vote en temps réel.

c. Suivez le rythme de la hausse des appareils intelligents connectés au réseau.

d. Assurez-vous que les informations confidentielles des invités/clients et les transactions financières sont protégées contre les attaques.

e. Conformez-vous aux réglementations PCI DSS (États-Unis) et RGPD (UE).

5. Santé



Description : Ensemble d'hôpitaux, de cabinets de médecins et de centres médicaux utilisant des réseaux et des technologies disparates pour offrir des services de santé.

a. Connectez les établissements de santé publics et privés pour partager les informations médicales critiques.

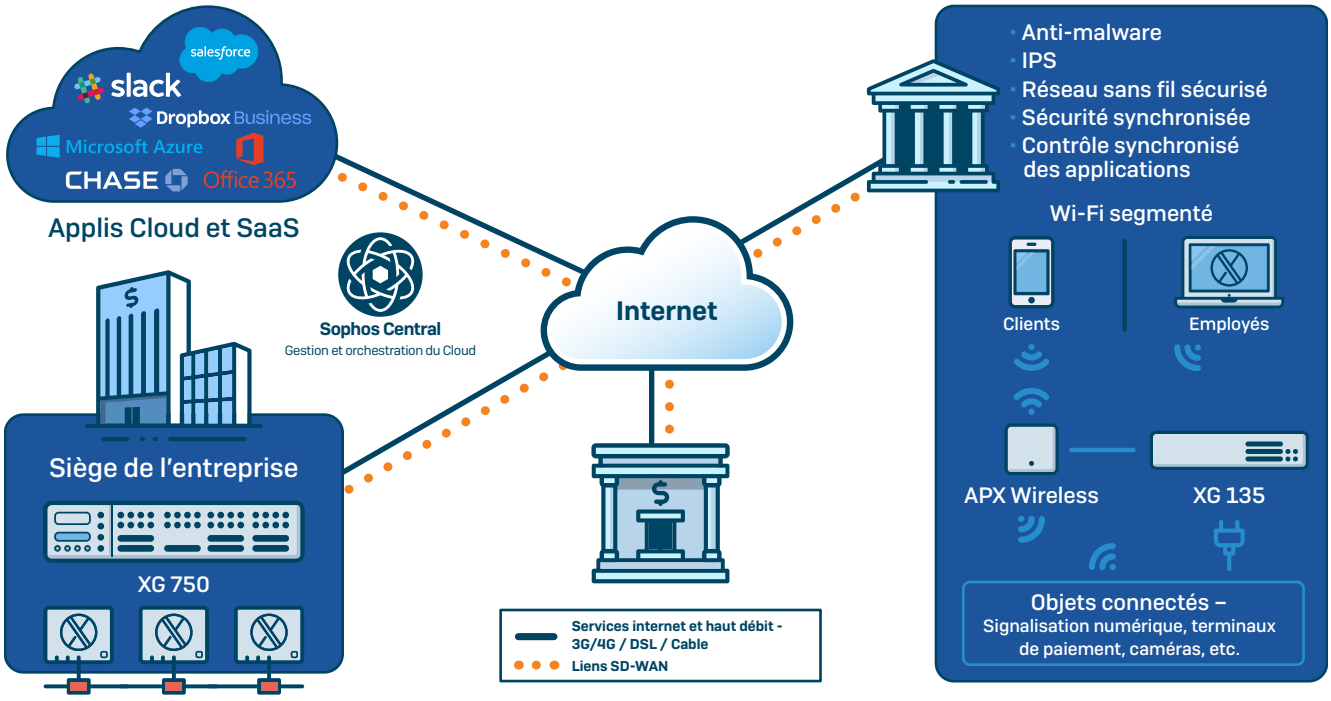
b. Suivez le rythme de la hausse du nombre d'appareils médicaux et d'appareils connectés.

c. Facilitez l'utilisation de nouvelles technologies et applications de santé sur le réseau, comme la télésanté.

d. Déployez de nouveaux établissements de santé ou ajoutez rapidement des cabinets existants au réseau en utilisant un déploiement Zero-Touch.

e. Conformez-vous aux réglementations HIPAA (États-Unis) et RGPD (UE) qui exigent la transmission sécurisée des données numériques confidentielles des patients (ePHI - Electronic Protected Health Information).

6. Finance



Description : Les institutions comme les banques, les coopératives de crédit et les sociétés de courtage qui offrent des services financiers aux particuliers et aux entreprises.

a. Connectez les succursales locales, régionales et nationales qui partagent chaque jour de grandes quantités d'informations sensibles sur les clients.

b. Protégez les données personnelles et professionnelles et les transactions financières contre les cyber menaces.

c. Suivez le rythme de la hausse rapide des objets connectés, tels que les distributeurs automatiques de billets et les caméras de sécurité.

d. Activez de nouvelles technologies et applications sur le réseau, telles que les services bancaires mobiles, les signatures électroniques, la signalisation numérique et les vidéos.

e. Conformez-vous aux réglementations PSD2, PCI DSS (États-Unis) et RGPD (UE).

Conclusion

Le panorama des réseaux distribués continue d'évoluer. Les technologies anciennes telles que le MPLS qui connectaient auparavant de nombreux sites sur de vastes régions géographiques ne sont plus la meilleure solution. Les entreprises d'aujourd'hui se tournent vers le SD-WAN qui offre à moindre coût une plus grande flexibilité, davantage de contrôle sur les applications et une meilleure agilité.

Les pare-feu XG de Sophos avec capacités SD-WAN intégrées vous permettent de connecter vos sites distants ou vos succursales, de distribuer des applications Cloud et SaaS critiques et de partager des données et des informations tout en orchestrant le tout depuis le Cloud et dans une seule solution. Et vous avez l'assurance d'être protégé par un leader de l'industrie en matière de cybersécurité.

Pour en savoir plus sur le SD-WAN et sur Sophos XG Firewall, RDV à la page www.sophos.fr/sd-wan.

Pour en savoir plus sur le SD-WAN et sur Sophos XG Firewall, visitez www.sophos.fr/sd-wan

Équipe commerciale France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

20-12-18 UC-FR (MP)

SOPHOS