DOSSIER THÉMATIQUE :

Les sites de vos succursales sont-ils une porte ouverte aux cyberattaques ?

Pourquoi une exposition accrue, des ressources limitées et des coûts croissants exigent une solution SD-Branch sécurisée

Résumé

Les méthodes traditionnelles de déploiement et de maintien de la sécurité des sites des succursales sont devenues inefficaces, coûteuses et ingérables. Une solution SD-Branch dans les succursales peut constituer la clé de voûte pour une sécurité illimitée dans les environnements d'entreprises distribuées.

Une explosion des points d'exposition

Les chercheurs spécialistes en menaces des Capture Labs de SonicWall ont enregistré 9,9 milliards d'attaques de logiciels malveillants en 2019. Au cours des cinq dernières années, les cybercriminels ont submergé les organisations d'un volume considérable. Leur objectif était simple : ratisser aussi large que possible pour récolter le fruit de leurs attaques. Au fur et à mesure de l'évolution des cyberdéfenses, les attaques sont devenues plus ciblées, avec des degrés de réussite plus élevés.

En outre, le paysage du réseau et de la sécurité subit une transformation numérique avec l'explosion des appareils mobiles et des dispositifs IdO. Par conséquent, les entreprises ont tendance à s'appuyer sur des clients mobiles, créant des réseaux dédiés aux appareils mobiles en priorité. Un autre catalyseur de ce changement est le passage au cloud et l'adoption des applications cloud. Alors que les applications critiques comme MS Office migrent dans le cloud et que les entreprises utilisent des applications cloud comme Salesforce ou Workday pour leurs tâches quotidiennes, il est devenu essentiel de sécuriser ces applications cloud. Cette transformation numérique stimule la demande d'appareils haute performance qui peuvent suivre les demandes croissantes de données.

Le coût toujours croissant de la connectivité

Les bureaux ou agences mobiles s'appuient fortement sur des applications à haut débit pour effectuer de simples activités quotidiennes, comme regarder des vidéos en streaming ou d'autres contenus ou travailler sur Office 365. Parmi ces applications à haut débit, certaines peuvent être critiques pour l'entreprise, tandis que d'autres ne le sont pas. Il est essentiel de séparer ce trafic efficacement ou il devient excessivement cher : imaginez devoir acheminer tout le trafic des succursales via des liaisons MPLS coûteuses vers le siège social de l'entreprise.

Heureusement, les dépenses peuvent être réduites en utilisant un accès Internet à faible coût pour le trafic de données non critiques, tandis que le trafic de données essentielles pour l'entreprise peut être hiérarchisé grâce au mécanisme de sélection dynamique des chemins. Cependant, certaines de ces applications, essentielles au fonctionnement d'une entreprise ou d'une succursale distribuée, nécessiteraient une connectivité redondante pour assurer une disponibilité constante.

Une façon d'assurer une connectivité redondante pour ces branches est d'avoir une solution qui offre une disponibilité élevée et des réseaux locaux performants avec équilibrage de charge WAN. Pour cela, il est possible d'avoir recours à la technologie de mise en réseau programmable dans un réseau étendu (SD-WAN).

En utilisant un accès Internet à faible coût (haut débit, 3G/4G/LTE, fibre), les entreprises peuvent remplacer de manière rentable les technologies de connexion WAN coûteuses (MPLS, par exemple) par la technologie SD-WAN.

Cependant, fournir ce service tout en gérant l'ensemble de la solution de sécurité réseau à partir d'un seul écran devient souvent compliqué.

Lutter contre la diminution des ressources

La sécurité conventionnelle est de plus en plus chère et la pénurie de personnel formé de plus en plus grande. Les ressources budgétaires et humaines limitées ne peuvent tout simplement pas suivre, laissant place à un déficit en matière de cybersécurité.

Les produits multipoints compliquent le déploiement, la configuration, la gestion et le dépannage de la solution pour les succursales. Disposer d'une pile de sécurité de bout en bout peut unifier les pare-feu, les commutateurs, les points d'accès, la sécurité dans le cloud et les clients terminaux afin de fournir une gestion sur un seul et même écran qui amplifie la visibilité et le contrôle entre les produits. Cette pile de sécurité de bout en bout offre une sécurité forte et unifiée.

Il est essentiel de changer la façon dont vous entretenez les réseaux. Vous pouvez suivre cette transformation numérique en fournissant une sécurité solide. Si vous ne fournissez pas de sécurité unifiée, les organisations auront du mal à gérer et contrôler le nombre croissant d'appareils sur le réseau. Les menaces ne seront pas identifiées et les entreprises seront obligées d'adopter une approche réactive plutôt que proactive.

En outre, le déploiement à grande échelle peut être difficile sans technologies telles que le déploiement sans intervention. Les techniciens devront se rendre dans ces succursales pour configurer manuellement chacun de ces appareils, ce qui augmente le coût global et le temps passé à déployer la solution dans toutes les succursales, peut-être à l'échelle mondiale.

En outre, les succursales autant que le siège social doivent fournir un accès sans fil sécurisé qui offre une expérience utilisateur haute performance et supérieure. En raison de l'omniprésence du Wi-Fi, les employés comme les clients attendent des performances Wi-Fi fiables et rapides.

Pourquoi vous avez besoin d'une solution SD-Branch

Aujourd'hui, l'évolution de la technologie au niveau de la succursale est essentielle. Les succursales traditionnelles ne peuvent pas suivre les demandes croissantes provenant de la multiplication des appareils mobiles et des dispositifs IdO. La prolifération des appareils rend la gestion et la sécurité difficiles, car ils peuvent avoir besoin de politiques différentes. Avoir une politique unifiée sur votre LAN et votre WAN depuis un seul et même écran (SPOG) devient essentiel.

En outre, la gestion SPOG peut fournir des analyses riches et complètes dans tout l'écosystème de sécurité. À mesure que l'adoption du cloud s'accélère, la connectivité WAN entre les succursales doit être conçue intelligemment pour tirer parti de liens Internet moins onéreux par rapport à des liens MPLS plus coûteux, et permettre un déploiement sans intervention.

Cela induit une agilité opérationnelle. Les entreprises peuvent rapidement développer et déployer des dispositifs avec une capacité de déploiement sans intervention, éliminant ou réduisant le besoin en personnel informatique qualifié pour visiter plusieurs succursales afin de configurer et déployer ces solutions. Pour assurer la continuité, l'intégration et l'évolutivité, les organisations doivent rechercher de manière optimale une gestion SPOG rationalisée avec des services provenant d'un seul fournisseur.

Une solution SD-Branch augmente le SD-WAN pour fournir le niveau supérieur de connectivité et de flexibilité. SD-Branch transforme la technologie SD-WAN en une solution sur mesure pour les déploiements dans les succursales. Cette solution ajoute plus de fonctionnalités et va au-delà de la connectivité entre les succursales. SD-Branch englobe le SD-WAN, la connectivité LAN et la sécurité. En outre, le déploiement sans intervention et la gestion SPOG réduisent les besoins en personnel informatique, ce qui limite encore davantage les coûts opérationnels.

Conclusion

Les entreprises distribuées éprouvent des difficultés à sécuriser les sites des succursales en raison de l'augmentation des points d'exposition, des ressources limitées et de la hausse des coûts. Tout cela contribue à un déficit croissant en matière de cybersécurité.

Une solution efficace associe l'agilité de SD-Branch à la sécurité de bout en bout, la segmentation du réseau et la conformité. Cela permet des politiques unifiées dans l'écosystème du réseau, fournissant des contrôles de sécurité granulaires afin d'identifier et d'empêcher les attaques les plus furtives et inédites d'aujourd'hui qui visent à compromettre votre réseau.

SonicWall considère SD-Branch comme la clé de voûte de la sécurité illimitée à l'ère de l'hyper-distribution. La solution SonicWall SD-Branch sécurise la connectivité et transforme l'expérience utilisateur dans les succursales en fournissant une plateforme intégrée qui permet aux agences de profiter d'une connectivité moins chère (SD-WAN), d'avoir recours au BYOD, d'adopter des applications SaaS et de se connecter au siège social ou à d'autres succursales. Elle intègre le SD-WAN, le déploiement sans intervention, la gestion à écran unique, la visibilité unifiée et la détection des menaces, les pare-feu de nouvelle génération, les commutateurs sécurisés, les points d'accès sans fil, la sécurité des terminaux et la sécurité des applications cloud.

En savoir plus : Lisez notre Présentation de la solution SD-Branch de SonicWall.

À propos de SonicWall

SonicWall offre une Boundless Cybersecurity pour l'ère de l'hyper-distribution et une réalité professionnelle où tout le monde est mobile, travaille à distance et sans sécurité. En connaissant l'inconnu, en offrant une visibilité en temps réel et en permettant de véritables économies. SonicWall comble le fossé commercial en matière de cybersécurité pour les entreprises, les gouvernements et les PME du monde entier. Pour en savoir plus, rendez-vous sur www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consultez notre site Internet pour plus d'informations.
www.sonicwall.com

ExecutiveBrief-AreYourBranchSites-US-VG-1980