SASE : sécurité des réseaux et du cloud dans votre entreprise distribuée

Les tendances telles que le travail hybride et le passage au multicloud voient les entreprises adopter des modes de travail distribués encore jamais vu. Cela veut dire que le périmètre de votre réseau, autrefois clairement défini, s'est transformé en une frontière disparate et en flux perpétuel, où la séparation entre l'interne et l'externe est devenue floue. Comment le protéger ? Le SASE a les réponses.

Les collaborateurs qui jonglaient entre bureau, télétravail et déplacements existaient déjà avant la COVID-19, mais la pandémie a rapidement amplifié leur nombre. Quatre-vingt-quinze pour cent des travailleurs déclarent maintenant vouloir des horaires de travail flexibles et 78 %[1] veulent une flexibilité quant à leur lieu de travail. Cela implique donc un changement dans la manière dont vous sécurisez utilisateurs et données. Il semble que les modes de travail hybrides ne soient pas prêts de disparaître.

Cela veut également dire que l'optimisation des coûts d'exploitation de vos bureaux doit devenir une priorité. L'adoption des technologies SD-WAN et SD-Branch doit pouvoir vous permettre d'accéder à une plus grande agilité et à une plus forte innovation sans pour autant vous exposer à des risques plus importants.
Le multicloud a pris encore plus d'ampleur ces dernières années, à mesure que la flexibilité des entreprises soit devenue une priorité. Les entreprises ont accéléré leur effort de réduction des infrastructures de datacenters de grande envergure et ont cherché des méthodes pour mieux gérer leurs dépenses et atteindre leurs objectifs de soutenabilité grâce à des modèles de consommation en cloud, tout en développant de nouvelles manières de traiter les données et d'offrir des expériences uniques aux utilisateurs.

Cela signifie également que les entreprises ont dû repenser l'infrastructure de réseau traditionnelle, où les centres de données pouvaient souvent constituer un obstacle à l'évolutivité ainsi qu'un poste de dépenses élevés. De nombreuses entreprises comprennent désormais l'intérêt d'adopter une approche centralisée de la sécurité du cloud, hébergé par un partenaire tiers, comme l'illustre si bien le SASE.

Challenges de l'entreprise distribuée

La dispersion géographique des utilisateurs se traduit par une prolifération des points d'accès. Dans une entreprise plus distribuée, ce qui était autrefois un périmètre de sécurité étroitement défini est maintenant réparti entre bureaux, cloud, domiciles, lieux de travail, et plus encore.

Tous ces travailleurs à distance accèdent à de plus en plus de données via l'Internet, ce qui les expose à davantage de sites web malveillants et à des violations potentielles de la sécurité de leurs données.
Vos différentes agences sont également exposées à des menaces venant du web contre lesquelles elles étaient auparavant protégées grâce aux réseaux MPLS traditionnels.

Vous devez vous assurer que les utilisateurs finaux soient protégés de manière constante et ne puissent accéder uniquement aux données et aux applications auxquelles ils doivent avoir accès, et cela, d'où qu'ils se connectent.

Le zéro trust garantit que seules les personnes autorisées peuvent accéder aux données appropriées et tire parti d'une visibilité approfondie pour dresser un tableau complet des menaces potentielles. Il vous montre ce qu'il se passe dans votre réseau et vous offre une gestion centralisée et cohérente de la sécurité.

orange™ Business

Votre checklist SASE

Le Secure Access Service Edge (SASE) intègre les dernières innovations en matière de réseau et de sécurité, notamment la sécurité multicloud et la sécurité réseau, dans une architecture de sécurité complète et systémique conçue pour protéger les entreprises distribuées. Il inclut le SD-WAN pour fournir une visibilité de bout en bout avec un trafic optimisé de l'Internet ou de réseaux privés vers vos ressources cloud et centre de données.

60 %

des organisations adopteront le zéro trust comme point de départ de leur stratégie sécurité d'ici 2025[2]

Alors qu'utilisateurs et données se retrouvent de plus en plus distribués et que l'Internet devient le nouveau WAN, le SASE peut vous aider à protéger votre entreprise distribuée :

- Protéger vos connexions réseau traditionnelles : vous devez encore et toujours protéger les données qui circulent entre vos bureaux et les centres de données principaux, et renforcer cette protection à l'aide d'une connectivité résiliente. Le SD-WAN et le ZTNA (Zero Trust Network Access) sont maintenant les réseaux les plus efficaces pour protéger le trafic des entreprises et le travail hybride.
- Protéger vos utilisateurs dans le cloud : Sites web malveillants, ingénierie sociale et cyberattaques traditionnelles signifient que vos connexions au cloud doivent être protégées. Cette protection doit être cohérente, quel que soit l'endroit où se trouvent les utilisateurs, et doit être basée sur l'identité numérique. Les passerelles internet sécurisées et le RBI (remote browser isolation ou isolation du navigateur à distance) peuvent vous proposer cette fonctionnalité.
- Protégez vos données dans le cloud : les données dans le cloud doivent être protégées contre les menaces internes et externes. La prévention des fuites de données (data leak prevention ou DLP) et les courtiers en sécurité d'accès au cloud (cloud access security brokers ou CASB) protègent vos données en s'assurant qu'elles ne sont pas téléchargées et exfiltrées des PC.
- Révisez votre modèle de confiance : assurez-vous que les personnes qui accèdent à vos données sont bien celles qu'elles prétendent être.

Des conseils pour protéger votre entreprise distribuée

Avec l'augmentation des modes de travail hybrides et l'usage du multicloud, vous êtes maintenant entouré d'applications, d'utilisateurs et de données. Cette nouvelle forme d'entreprise distribuée signifie que la traditionnelle sécurité du périmètre réseau ne suffit plus : dans un monde de cybermenaces de plus en plus sophistiquées, vous avez également besoin d'une réponse sophistiquée.

1. **Adoptez le zéro trust comme stratégie a l'échelle de votre entreprise.** La première étape est de vous assurer que votre approche zéro trust est cohérente au sein de toute votre organisation. Vous aurez besoin d'un responsable au sein de votre entreprise pour mener ce projet à bien. N'oubliez pas que la sécurité de votre entreprise repose sur son maillon de défense le plus vulnérable. Orange Cyberdefense peut vous fournir des experts consultants pour revoir votre posture de sécurité.

2. **Définir votre stratégie zéro trust.** Prenez des mesures pour améliorer votre position en matière de sécurité. Par exemple, mettre en place une stratégie de sécurité basée sur l'identité numérique qui limite l'accès à l'infrastructure et aux données. La segmentation du réseau dans le LAN/WAN et le cloud, ainsi que la segmentation des applications, peuvent vous aider à bien verrouiller l'accès. Un monitoring permanent et efficace des menaces et une maintenance tout au long du cycle de vie de votre infrastructure informatique sont essentielles.

3. **Commencez par l'accès à distance.** L'accès à distance est typiquement une priorité pour les entreprises. Orange Business travaille avec vous pour comprendre vos besoins d'accès à distance et mettre en œuvre une solution adaptée à vos besoins. Orange Business et Orange Cyberdefense peuvent s'occuper de gérer la solution pour vous afin que vous puissiez la déployer en tant que service, ou nous pouvons vous proposer une cogestion.

4. **Passez au SD-WAN.** Alors que l'usage du cloud par les entreprises augmente de jour en jour et qu'elles commencent à tirer parti de leur accès Internet pour la connectivité WAN, le SD-WAN vous donne une base concrète pour un réseau sécurisé. Une amélioration de la visibilité et l'automatisation facilitent la mise en œuvre cohérente de politiques de sécurité communes à l'ensemble de votre réseau. De surcroît, le SD-WAN offre une connectivité sécurisée entre les différents bureaux et le cloud. En tant que fournisseur expert en infogérance SD-WAN, Orange Business peut vous aider à éliminer le risque et la difficulté du déploiement et de l'exploitation d'un réseau SD-WAN et de son routage sous-jacent a l'aide de notre réseau mondial et de nos équipes de services sur le terrain.

5. **Vers le SASE de bout en bout.** C'est en réunissant les différents éléments de sécurisation du cloud tels que les courtiers en sécurité d'accès au cloud (CASB) et le SD-WAN que le SASE prend tout son sens. Travailler avec un fournisseur SASE expert comme Orange Business vous donne accès aux compétences et ressources nécessaires et vous permet de vous concentrer sur la gestion de votre entreprise. Orange Business et Orange Cyberdefense vous proposent les meilleurs services en matière de sécurité du cloud et de SD-WAN et offrent une expérience utilisateur final incomparable tout en réduisant la complexité et les risque lies à la sécurité.

6. **Protégez vos utilisateurs et données.** De nouvelles menaces pour la sécurité se manifestent sur Internet, des attaques réseau aux sites web malveillants, etc. Orange Cyberdefense peut vous aider à protéger vos données et vos utilisateurs grâce à un cloud sécurisé, afin que votre trafic Internet soit aussi sûr que l'était le trafic interne sur votre réseau MPLS.

7. **Intégrez votre réseau local dès le premier jour.** Assurez-vous que votre réseau local soit constamment mis à jour avec les dernières versions et les meilleures mesures de sécurité en utilisant un SD-LAN. Le zéro trust s'applique à l'ensemble des appareils de vos utilisateurs en passant par le réseau local de votre entreprise et jusqu'au cloud.

8. **Collaborez avec un partenaire pour gérer en partie vos services de sécurité.** Orange Business estime que la sécurité ne doit jamais être complètement sous-traitée, cette thématique relevant en effet d'une responsabilité collective Orange Cyberdefense peut vous aider dans des domaines clés de la sécurité tels que la conception et le déploiement, les audits ou la maintenance de vos équipements.

Découvrez comment Orange Business et Orange Cyberdefense peuvent vous aider a protéger votre entreprise distribuée avec le SASE sur www.orange-business.com/fr/enjeux/infrastructure-numerique-evolutive-reactive-securisee/sase-secured-access-service-edge

orange™ Business

Orange Cyberdefense

1. https://futureforum.com/research/leveling-the-playing-field-in-the-hybrid-workplace/ 2. https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio