Écrit par :

netskope

Conception d'une architecture SASE

pour les nuls®

Maîtrisez la sécurité dans le cloud

Gérez les principaux changements en matière d'applications, de données, de sécurité et de réseaux

Améliorez et préservez l'expérience utilisateur

Jason Clark
Lamont Orange
Steve Riley

Édition spéciale Netskope

À propos de Netskope

Netskope, le leader du SASE, connecte rapidement et en toute sécurité les utilisateurs directement à Internet, à n'importe quelle application et à leur infrastructure depuis n'importe quel appareil, sur le réseau ou en dehors. Grâce à l'intégration native des services CASB, SWG et ZTNA dans une seule plateforme, Netskope fournit une solution omniprésente rapide, centrée sur les données et « cloud smart », tout en favorisant un Internet citoyen et en offrant un coût total de possession plus faible. Pour en savoir plus, rendez-vous sur le site www.netskope.com.

Nous tenons à remercier un certain nombre de personnes qui ont rendu possible la publication de ce livre :

Chez Netskope : Amanda Anderson, Mike Anderson, Chad Berndtson, James Christiansen, Tom Clare, Mark Day, David Fairman, Maxwell Havey, Scott Hogrefe, Kathy Jacobsen, Greg Mayfield, Mariesa Milan, Sasi Murthy, Krishna Narayanaswamy, Lauren Polito, Kate Reid, Zoe Revis, Brian Tokuyoshi

Chez Evolved Media : Karen Queen, Evan Sirof, Lauren Wagner, Dan Woods

Conception d'une architecture SASE

Édition spéciale Netskope

par Jason Clark, Lamont Orange, et Steve Riley

pour les nuls®

Conception d'une architecture SASE pour les Nuls®, une édition spéciale Netskope

Publié par
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-85520-0 (pbk) ; ISBN 978-1-119-85521-7 (ebk)

Imprimé aux États-Unis d'Amérique

10 9 8 7 6 5 4 3 2 1

Remerciements de l'éditeur

Cet ouvrage a été réalisé avec la participation des personnes suivantes :

Rédacteur projet : Elizabeth Kuball

Rédacteur chargé des acquisitions : Ashley Coffey

Responsable éditorial : Rev Mengle

Représentant du développement commercial : William Hull

Éditeur de production : Vivek Lakshmikanth

Assistance spéciale : Nicole Sholly

Introduction

Vos employés, partenaires et clients utilisent de plus en plus le cloud à la place de réseaux et de datacenters privés. La sécurité ne peut pas entraver leur mode de fonctionnement. Pendant ce temps, vous et vos collègues chefs d'entreprise vous efforcez de réaligner la sécurité sur un environnement qui, si vous utilisez des outils de sécurité traditionnels, échappe à votre contrôle. Cet équilibre entre sécurité et expérience utilisateur est difficile à atteindre en temps « normal », mais aucun catalyseur n'a mis les organisations au défi comme la pandémie de COVID-19, qui a entraîné l'adoption du télétravail pour des millions de personnes.

La complexité du paysage de la sécurité a mis au défi même les meilleures équipes spécialisées et augmenté le risque de mauvaises configurations et de failles. Les produits, services et messages industriels contradictoires font qu'il est difficile pour les décideurs de ce domaine de saisir les opportunités tout en remaniant la sécurité pour répondre à leurs besoins.

Une nouvelle architecture réseau et de sécurité appelée *Secure Access Service Edge* (SASE, prononcer « *sassy* ») montre la voie à suivre. Les NG-SWG (Next-Generation Secure Web Gateways), les CASB (Cloud Access Security Brokers) et les principes Zero Trust sont des éléments constitutifs essentiels de l'architecture SASE qui combine des services réseau clés et des services de sécurité dans un même *système* unifié afin de protéger les intérêts commerciaux et la facilité d'utilisation du cloud. Mais comment organiser tout cela de la bonne manière et dans le bon ordre ? C'est là que ce livre entre en jeu.

À propos de ce livre

Ce livre peut vous aider à élaborer une feuille de route pour l'implémentation de projets de gestion du réseau et de la sécurité qui produiront des résultats positifs et progressifs à court terme, tout en ouvrant la voie à un avenir résilient et sécurisé donnant la priorité au cloud. Il vous permet de comprendre les tenants et les aboutissants du SASE loin du bruit marketing émanant des soi-disant fournisseurs de SASE ; et vous donne les moyens d'anticiper vos investissements en matière de sécurité et de réseau afin de vous adapter aux changements inévitables de la manière la plus simple et la plus rentable possible.

Quelques suppositions idiotes

Vous connaissez bien l'Internet. Vous savez qu'il abrite une grande variété d'outils numériques basés sur le cloud que les personnes utilisent pour leurs besoins professionnels et personnels (et qui sont utilisés sans l'implication, et encore moins l'approbation, des équipes de sécurité et informatiques). Vous savez également que le cloud peut être un endroit dangereux où les informations d'identification et les données des particuliers et des entreprises peuvent faire l'objet d'attaques. Enfin, vous souhaitez relever ce défi pour votre entreprise, vos employés, vos actionnaires, vos clients et vos partenaires commerciaux.

Icônes utilisées dans ce livre

Nous utilisons des icônes dans la marge pour attirer l'attention sur les informations importantes. Voici leur signification :

CONSEIL

Tout le contenu en regard de l'icône *Conseil* est un raccourci pour faciliter une tâche spécifique.

RAPPEL

L'icône *Rappel* signale les faits qu'il est particulièrement important de connaître.

JARGON TECHNIQUE

Lorsque nous proposons des informations très techniques que vous pouvez ignorer sans risque, nous utilisons l'icône *Jargon technique*.

ATTENTION

Tenez bien compte de tout ce qui se trouve en regard de l'icône *Attention* pour vous épargner des maux de tête.

Au-delà de ce livre

Bien que ce livre regorge d'informations, si vous vous retrouvez à la fin à vous demander « Où puis-je en savoir plus ? », rendez-vous sur `www.netskope.com`.

DANS CE CHAPITRE

- **Reconnaître comment la sécurité a changé à l'ère du cloud**
- **Identifier les nouveaux problèmes découlant de pratiques de sécurité antérieures au cloud**
- **Découvrir le SASE et la façon dont il permet aux entreprises d'utiliser le cloud**
- **Créer une solution durable grâce à une architecture SASE qui fonctionne**
- **Séparer la valeur du SASE du bruit marketing**

Chapitre 1
La vision du SASE pour la sécurisation des entreprises Cloud-First

Le terme *cloud* est si souvent utilisé qu'il est parfois difficile de comprendre ce qu'il signifie. Du point de vue des applications, et en termes très simplifiés, le terme *cloud* peut faire référence aux éléments suivants :

- **Cloud privé :** applications dans votre datacenter.
- **Cloud public :** on entend parfois beaucoup de choses par là, notamment l'IaaS (Infrastructure as a service) et le PaaS (Platform as a service), mais pour simplifier, pensez simplement au cloud public comme des applications disponibles sur l'Internet public.
- **Cloud privé virtuel :** applications privées accessibles à partir du cloud public.

- **SaaS (Software as a service) :** applications hébergées par un fournisseur tiers et accessibles sur Internet.

Cette utilisation familière du mot *cloud* peut rendre difficile l'évaluation des options et de leur relation avec vos besoins spécifiques. Commencez par comprendre ce que vous devez faire en matière de sécurité. Cette étape vous permettra de clarifier les problèmes et d'identifier les fonctionnalités dont vous aurez besoin dans toutes vos interactions avec le cloud.

Dans ce chapitre, vous découvrirez comment le cloud a changé les exigences de sécurité, pourquoi la sécurité antérieure au cloud est désormais obsolète, pourquoi les approches réseau traditionnelles comme le *hairpinning* ne fonctionnent pas, comment le SASE (Secure Access Service Edge) peut permettre à vos employés de travailler de manière sûre et productive dans le cloud, et les facteurs déterminants de la meilleure architecture SASE.

FIN DU PHÉNOMÈNE DE NICHE

Les vulnérabilités liées au cloud ne peuvent plus être considérées comme un phénomène de niche. À compter de 2021 :

- Le nombre d'applications cloud utilisées par les entreprises a augmenté de 20 % par rapport à l'année précédente. Selon un rapport publié en février 2021 par Netskope, les entreprises comptant entre 500 et 2 000 employés utilisent désormais, en moyenne, 664 applications cloud distinctes par mois.
- 61 % des téléchargements de logiciels malveillants peuvent être attribués au stockage dans le cloud et aux applications collaboratives en décembre 2020, contre 48 % en janvier 2020, selon le rapport Netskope.
- Selon ce même rapport, 55 % des sessions sont liées aux applications et aux services cloud dans le trafic web.
- Enfin, ce rapport montre que 83 % des utilisateurs accèdent à des applications personnelles sur des appareils gérés par l'entreprise. Voici donc la question de sécurité urgente à laquelle vous devez répondre : comment permettre à votre entreprise de tirer le meilleur parti de tout ce que le *cloud* peut offrir en termes de flexibilité, de gestion des coûts et d'opportunités commerciales, tout en garantissant en permanence la sécurité de vos utilisateurs, de vos clients, de vos données et de vos autres actifs précieux ?

Comment le cloud a changé la sécurité et les réseaux

Il fut un temps où les datacenters des entreprises étaient de puissantes forteresses dans le monde des affaires. Les entreprises ont érigé ces citadelles numériques, puis conçu et déployé des applications professionnelles à l'intérieur de ces murs. À l'intérieur de la forteresse, les entreprises ont mis en place des réseaux privés qui relient les personnes aux données, qu'il s'agisse du personnel du siège, des employés des sites distants ou des travailleurs itinérants qui voyagent à travers le monde.

Comme dans tous les grands châteaux forts, un périmètre était clairement délimité à l'aide d'un mur et d'une porte gardée. L'accès aux contrées sauvages d'Internet au-delà de la porte était strictement réglementé. Les gardiens pouvaient surveiller le trafic le long des routes protégées du réseau, laissant entrer les gens vertueux, écartant tout ce qui est suspect, et intervenant au premier signe de problème. Chaque échange avec le monde extérieur était contraint de faire des allers-retours dans les limites étroites du réseau privé.

Tout d'abord, un filet, puis un torrent, d'utilisateurs professionnels se sont tournés vers des applications basées dans le cloud. Les applications basées sur le cloud, pour les réseaux sociaux, la communication, la collaboration, le traitement des informations sur les ventes, la finance, le marketing et la relation client, étaient tout simplement meilleures que les solutions proposées en interne. Les entreprises et même les organismes publics, qui sont d'habitude plutôt lents à adopter de nouvelles technologies, ont alors suivi la tendance. Aujourd'hui, les entreprises privilégient les applications SaaS et ont adopté des stratégies radicales *Cloud-First* qui imposent de résoudre les problèmes métiers à l'aide de solutions cloud et de transférer les systèmes d'entreprise essentiels vers le cloud.

Les choses ont changé lorsque le cloud a commencé à proposer de nouvelles applications puissantes. Les personnes, les appareils et les applications sont mobiles, que ce soit sur ou en dehors de votre réseau. Les produits SaaS offrent des fonctionnalités fantastiques aux entreprises, plus rapides et meilleures que les approches précédentes qui nécessitaient de longs délais de développement et l'acquisition de matériel et de logiciels.

À la fin de la dernière décennie, les dépenses consacrées aux activités cloud ont augmenté de manière significative pour dépasser de loin le rythme de tous les autres postes des budgets informatiques, selon le Synergy Research Group. Selon le cabinet Gartner, d'ici 2024, plus de

45 % des dépenses informatiques consacrées à l'infrastructure système, aux logiciels d'infrastructure, aux logiciels applicatifs et à l'externalisation des processus métiers passeront des solutions traditionnelles au cloud, faisant de ce dernier l'une des forces les plus perturbatrices du marché informatique depuis les débuts de l'ère du digital.

Pourtant, bon nombre de ces outils basés sur le cloud échappent à la visibilité et au contrôle des départements IT. Du point de vue de la sécurité, c'est inquiétant. Mais la sécurité ne se limite pas à la protection des applications cloud.

La sécurité consiste également à fournir toute la protection nécessaire lorsque l'ensemble de votre personnel travaille à distance. Où qu'ils soient, vos utilisateurs doivent être protégés contre les attaques et bénéficier de garde-fous pour assurer la sécurité des données et des applications. Et du point de vue de la gestion réseau, l'expérience doit être non seulement sûre, mais aussi fonctionnelle. La sécurité ne peut pas être un obstacle à la productivité indéniable que les utilisateurs réalisent lorsqu'ils peuvent utiliser le cloud pour accomplir plus de tâches, plus rapidement, où qu'ils soient.

Et puis il y a les informations. Les données (qu'il s'agisse de la propriété intellectuelle, des chiffres de vente ou des numéros de carte bancaire des clients) sont un trésor précieux pour votre entreprise, peut-être plus précieux que les produits que vous vendez. Le fait que la sécurité informatique fasse la une des journaux n'est pas surprenant ; et quand c'est le cas, les nouvelles sont rarement bonnes. Puisque les données, les applications et les personnes évoluent pour la plupart dans le cloud, les anciennes techniques de sécurité développées pour les datacenters on-premise et autres infrastructures traditionnelles ont du mal à suivre. Le monde a connu une vague croissante d'attaques de la part de divers hackers utilisant des techniques sophistiquées pour faire des ravages et exploiter les vulnérabilités des applications cloud et de leur mode d'accès.

La transition vers le cloud n'a été ni facile ni sans heurts. Les anciennes routes qui traversent le réseau du datacenter sont parsemées d'obstacles, de désagréments et d'inefficacités qui ralentissent la productivité, frustrent les utilisateurs et compromettent la sécurité. Les applications basées dans le datacenter font pâle figure face aux applications SaaS en termes de productivité, d'expérience utilisateur et de commodité. Les améliorations indispensables apportées par le SaaS ont permis aux vendeurs de vendre davantage, aux spécialistes du marketing d'amplifier leurs messages, aux services des ressources humaines de trouver les meilleurs candidats et aux développeurs de produits de travailler plus

rapidement. Renoncer au SaaS reviendrait à renoncer à une productivité sans précédent. Aucune entreprise ne souhaite cela.

Le problème était que ces applications SaaS nécessitaient des données internes pour pouvoir être exploitées, alors qu'elles se trouvaient en dehors des murs de l'entreprise. Elles n'étaient donc pas contrôlées ou protégées par le département chargé de la sécurité. Ce dernier, sachant qu'il n'a que très peu de contrôle sur ce qui se passe dans le cloud, avait alors deux choix : refuser l'utilisation des données ou fermer les yeux. C'est ce que l'on appelle aujourd'hui le *Shadow IT*, où des utilisateurs, voire des services entiers, contournent le département IT et de la sécurité pour utiliser des outils SaaS comme Salesforce et Google Docs, ainsi que des outils de partage de fichiers volumineux comme Dropbox, qui sont pratiques, mais non approuvés pour un usage professionnel. Le Shadow IT existe depuis de nombreuses années, mais son utilisation (et ses dangers) s'est accélérée grâce à l'adoption du cloud. Les professionnels de la sécurité, avec leurs boîtes à outils conçues pour les datacenters d'entreprise et l'ancienne façon de surveiller et de contrôler les applications, se retrouvent dans une véritable impasse.

RAPPEL

La sécurité « ancienne formule » oblige toujours à faire des compromis : les choix visant à optimiser certains standards, comme la vitesse ou la flexibilité, se font au détriment d'autres, notamment la sécurité. Le SASE, s'il est bien implémenté, *permet d'agir à ce niveau*. Il permet aux personnes les plus proches du problème d'innover et de surmonter les obstacles grâce à la technologie, de manière sécurisée et structurée, tout en aidant les responsables informatiques à mieux comprendre leur activité.

Les problèmes de sécurité avant l'ère du cloud

L'utilisation des outils, techniques et technologies de sécurité antérieurs à l'ère du cloud reste répandue. L'infrastructure informatique de votre propre entreprise est probablement concernée par cet état de fait, qui crée une situation dans laquelle beaucoup de solutions de sécurité sont disponibles, mais le résultat est tout sauf sûr ou efficace. Les problèmes persistants relèvent généralement de l'une des deux catégories suivantes : une mauvaise approche ou l'absence totale d'approche stratégique.

La mauvaise approche

L'un des avantages perçus d'un datacenter d'entreprise et de l'efficacité de sa sécurité était qu'il permettait de conserver les actifs numériques d'une entreprise dans un endroit unique et sûr. Une entreprise pouvait alors créer son propre réseau privé pour connecter les employés du siège

social, ainsi que ceux des sites distants, et contrôler leur accès aux données dont ils avaient besoin dans le datacenter.

RAPPEL

Les entreprises ont toujours besoin de datacenters. Mais aujourd'hui, le datacenter n'est que l'un des nombreux sites utilisés par les utilisateurs et les données. Il n'occupe plus une place centrale pour les besoins métiers ou ne fait plus office de point de contrôle de sécurité unique.

Les systèmes de sécurité des datacenters sont généralement des appliances, c'est-à-dire des boîtiers physiques connectés au datacenter pour remplir des fonctions bien précises. Au fil des années, les entreprises ont acheté des systèmes de sécurité auprès de centaines de fournisseurs. En 2021, l'entreprise moyenne a acheté et déployé des dizaines de produits de sécurité. Dans la majorité des cas, ces produits n'ont pas été conçus pour fonctionner ensemble. Il est pratiquement impossible pour le personnel de sécurité d'intégrer tous ces systèmes dans une solution de sécurité orchestrée et adaptative capable d'appliquer des stratégies qui prennent en charge les applications cloud et les télétravailleurs.

ATTENTION

La diversité des systèmes entraîne souvent un chaos au niveau des consoles (et peut-être même des débats sur qui se sert de quelle console). Votre personnel chargé de la sécurité et du réseau peut être confronté à des dizaines de consoles différentes, chacune avec ses propres priorités et toutes demandant une attention particulière. Il peut s'avérer impossible d'avoir une vue d'ensemble ou de comprendre une situation particulière lorsque vous devez diagnostiquer un problème urgent. Les processus de sécurité de ce type sont également réactifs et s'appuient souvent sur des journaux de logs pour reproduire et diagnostiquer les événements. Pire, cet imbroglio de systèmes empêche de créer une infrastructure bien organisée et plus sécurisée. Vous ne pouvez obtenir cette organisation et cette sécurité qu'en créant un système de règles détaillées, pour maintenir automatiquement la sécurité dans la très grande variété d'interactions numériques qui se produisent.

RAPPEL

Le rôle du département chargé de la sécurité n'est pas seulement de prévenir les menaces. Il doit également identifier les outils qui permettent à votre entreprise de travailler plus rapidement et plus efficacement, notamment avec des effectifs décentralisés. Il doit donner la priorité à la protection des utilisateurs et des données, mais doit aussi s'adapter en temps réel pour suivre l'évolution rapide des exigences. Cela signifie offrir aux utilisateurs une expérience de travail fluide et productive, où qu'ils se trouvent, en leur permettant d'accéder aux données dont ils ont besoin avec des outils qui leur assurent productivité et réussite .

L'absence totale d'approche

Vos utilisateurs sont partout, et les réseaux d'aujourd'hui doivent être conçus dans cette optique. Essayer de forcer à maintes reprises tout le trafic d'un utilisateur à passer par les nombreux services de sécurité du datacenter étouffe la productivité. (Les professionnels de la sécurité et des réseaux appellent parfois cela le *hairpinning*, c.-à-d. une tactique qui oblige les utilisateurs à ralentir et à changer de cap en permanence au lieu de suivre la voie déjà tracée). Le *hairpinning* se traduit par des systèmes d'entreprise moins utilisables, des performances considérablement réduites et des utilisateurs frustrés.

Quelle est l'ampleur du défi que représente le contrôle de ce nouvel environnement ? Voici un exemple : le National Institute of Standards and Technology (NIST) est mandaté par le Congrès américain pour fournir aux organisations des conseils en matière de cybersécurité. Le NIST a publié un framework de cybersécurité qui identifie 400 points de contrôle à prendre en compte pour sécuriser toute application dans votre organisation. Ce chiffre est probablement sous-évalué, car il suppose que tout (utilisateur, données, application et réseau) réside on-premise, alors que ce n'est plus le cas.

L'énorme éventail de contrôles dont vous disposez pour les personnes et les services au sein de votre réseau n'est pas disponible pour vos systèmes de sécurité lorsqu'il s'agit d'applications SaaS. Votre stratégie doit consister à sécuriser un paysage beaucoup plus vaste, en temps réel, et à le faire en utilisant seulement trois points de contrôle :

- Les données, dont vous êtes propriétaire, qui entrent et sortent des applications SaaS
- L'identité de chaque utilisateur qui accède à ces applications
- L'approbation selon que votre entreprise fait affaire ou non avec l'entité externe

RAPPEL

La clé de la réussite de la sécurité du cloud réside dans le réajustement de vos objectifs. Les systèmes de sécurité du passé étaient largement basés sur le contrôle de l'accès. Ils incarnaient en quelque sorte les murs et les gardiens du château. Cette approche de type « château fort » ne fonctionne plus. Pour assurer la sécurité dans le cloud, il faut se concentrer non pas sur l'accès, mais sur l'activité : qui fait quoi, comment les applications sont utilisées, quelles données sont en mouvement. Si la métaphore du château a atteint ses limites pour vous, pensez plutôt à un match de basketball : il est temps de faire passer votre sécurité d'une défense de zone basée sur le périmètre à une défense d'homme à homme basée sur l'activité.

JARGON TECHNIQUE

Les systèmes de sécurité plus anciens savent généralement où se dirige un utilisateur sur Internet. Mais l'application SaaS qu'ils utilisent peut elle-même s'appuyer sur des dizaines, des centaines, voire des milliers de ressources supplémentaires pour alimenter la page web que votre utilisateur consulte. Pour assurer la sécurité dans le cloud, vous devez connaître ces détails. Vos outils existants ne permettent pas de déchiffrer le protocole TLS (Transport Layer Security), ce qui leur permettrait de voir ce qui se passe dans le trafic de communication de l'utilisateur avec cette application. Ces outils ne peuvent pas non plus repérer certaines connexions d'API que l'application SaaS utilise pour échanger des informations avec d'autres ressources inconnues afin de créer un environnement complet pour l'utilisateur. Sans ce type d'informations, vous ne pouvez jamais être certain que vos données sont sûres ou que ce que votre utilisateur voit provient d'une source légitime.

Définition du SASE

D'un côté, le SASE signifie déplacer les contrôles du périmètre de sécurité du réseau vers le cloud, tout en rendant ces contrôles plus rapides, plus sensibles aux applications et aux utilisateurs, et davantage centrés sur les données.

De l'autre, le SASE constitue une nouvelle stratégie architecturale pour la sécurité et les réseaux que votre organisation doit s'efforcer d'implémenter. Le SASE tient compte du fait qu'un monde centré sur le cloud nécessite un modèle actualisé de sécurité et de mise en réseau. Il tient également compte des façons fondamentales dont la sécurité, les réseaux, les applications et la protection des données se sont tous transformés.

Sur le plan fonctionnel, le SASE comprend un ensemble de services de sécurité et de mise en réseau intégrés et imbriqués, conçus et fournis non seulement pour permettre aux utilisateurs d'accéder au cloud, mais aussi pour surveiller en permanence leurs activités, leurs appareils et les applications qu'ils utilisent, afin que les données puissent être sécurisées à tout moment, à chaque point d'accès, sans pour autant sacrifier l'expérience utilisateur. Heureusement, les fondements de votre architecture de sécurité SASE peuvent être déployés dès aujourd'hui, par étapes successives (voir le chapitre 5).

ATTENTION

L'une des caractéristiques du SASE est que chaque aspect de cette architecture de sécurité est spécialement conçu pour être utilisé dans et avec le cloud. Elle ne réutilise pas les appareils ou le code destinés aux datacenters. Et vous savez déjà pourquoi : les services de sécurité pour les datacenters visent principalement à contrôler l'accès. Ils ne parlent

pas le langage natif du cloud, qui est riche en nuances et en informations destinées à décrire les connexions entre les points et à présenter les données contenues dans le flux du trafic entre les points. Gardez cela à l'esprit lorsque vous évaluez les options de sécurité et de mise en réseau.

Le contexte est crucial et vous guide pour déterminer l'étendue et la richesse de cette nouvelle architecture de sécurité. Les facteurs contextuels du SASE sont les suivants :

- L'identité de l'utilisateur
- Le device utilisé pour demander l'accès
- L'emplacement à partir duquel l'accès est tenté
- L'identité des applications accessibles dans le cloud
- Les données demandées : ce qu'elles sont et où elles sont stockées
- Le comportement de l'utilisateur
- L'interaction avec l'application : ce que l'utilisateur essaie spécifiquement de faire

Ensuite, tout en réévaluant en permanence ce flux dynamique d'informations, le système de sécurité du SASE applique la sécurité en fonction de stratégies qui déterminent les éléments suivants :

- Le niveau de service et le type de services réseau à appliquer
- L'utilisation de types appropriés de chiffrement des données
- Le niveau de protection des données à appliquer pour éviter toute utilisation abusive
- Le niveau d'authentification à appliquer
- Si l'application nécessite l'utilisation de services de sécurité spécifiques et spécialisés, comme un Cloud Access Security Broker (CASB, Cloud Acces Security Broker), intervenant de manière intermédiaire dans l'activité.

RAPPEL

Oui, il se passe beaucoup de choses dans une architecture SASE. Mais lorsqu'il est réellement fonctionnel et correctement mis en œuvre, le SASE simplifie et améliore considérablement la qualité de votre sécurité et de votre connectivité réseau. Lorsque le SASE est bien implémenté, toutes ces choses se produisent en temps réel, y compris la gestion continue des risques. En déplaçant les services de sécurité hors de votre datacenter vers le cloud, plus près de vos points de vulnérabilité et de vos utilisateurs, vous bénéficiez, à tout moment, d'une meilleure visibilité et d'un contrôle plus ferme et permanent sur les événements et les utilisateurs. Le SASE aide les équipes chargées des réseaux et de la sécurité à

effectuer la transition vers les nouvelles applications et les nouvelles méthodes de travail, tout en protégeant l'accès aux anciennes applications on-premise.

Les avantages économiques du SASE

Les raisons d'adopter un modèle SASE pour la sécurité sont étroitement liées à la valeur que les entreprises ont largement reconnue dans l'adoption du cloud. Le cloud permet aux personnes et aux entreprises de travailler de manière plus efficace, collaborative, rapide, souple et rentable. Le SASE pérennise ces progrès.

Favoriser la croissance de l'entreprise dans le cadre de sa transformation digitale

La sécurité doit être comme les freins d'une voiture rapide. Elle est là pour permettre d'aller vite (car vous savez que vous pouvez vous arrêter si nécessaire) afin de pouvoir gérer les risques plus rapidement. Elle n'est pas là pour ralentir l'activité, ni pour empêcher la vitesse.

Vous ne pouvez pas effectuer une transformation digitale en toute sécurité sans transformer vos contrôles de sécurité. À l'heure où toutes les entreprises adoptent de nouvelles technologies pour accélérer leur croissance et se rapprocher de leurs clients, le département IT peut les aider de manière significative en déplaçant les contrôles de sécurité pour qu'ils suivent l'utilisateur et les données, éliminant ainsi une grande partie des frictions du processus. Offrez à vos utilisateurs les applications et les accès dont ils ont besoin, avec un coaching en temps réel sur la manière de les utiliser en toute sécurité.

Évolution au rythme des changements

Le cloud fournit des services essentiels à tous les aspects de votre activité, et de nouveaux cas d'utilisation apparaissent chaque jour. Votre entreprise a certainement approuvé certains services cloud pour ses utilisateurs. Et s'il existe un service cloud non approuvé qui permet de faire les choses mieux, plus rapidement et à moindre coût pour certaines personnes ou des organisations entières, il est fort probable qu'un membre de votre organisation l'utilise également. Celui-ci a contourné la sécurité, payé l'abonnement, téléchargé l'application et l'utilise tous les jours.

Réduction des coûts

RAPPEL

Voici un truisme souvent répété en matière de sécurité : « Si vous pensez que la sécurité coûte cher, essayez donc d'évaluer le coût d'une violation de la sécurité ». Selon une étude publiée par IBM et Ponemon, le coût total moyen d'une violation de données est de 3,86 millions de dollars. La plupart des entreprises réalisent qu'elles ont besoin de sécurité, mais elles apprécient rarement combien elles en ont besoin jusqu'à ce qu'elles rencontrent un problème.

La sécurité est souvent perçue comme un centre de coûts peu visible lorsqu'il fonctionne au mieux. La sécurité est en fait un facilitateur d'activité, mais même en mettant de côté ce véritable rôle, le budget de la sécurité, qu'il soit important ou limité, doit être dépensé judicieusement. Malheureusement, les dépenses judicieuses et efficaces en matière de sécurité restent un problème pour de nombreuses organisations.

Le SASE présente d'importants avantages en termes de rentabilité. Grâce à son approche hautement intégrée des services de sécurité, le SASE peut contribuer à réduire les dépenses d'investissement, en consolidant les capacités de nombreuses appliances de sécurité pour datacenters. Avec moins de systèmes à surveiller et à entretenir, le SASE réduit également les dépenses d'exploitation. La consolidation des fournisseurs, l'amélioration de la conception des réseaux et l'interaction efficace avec les fournisseurs de services cloud permettent de réaliser des économies supplémentaires.

Le SASE permet également de surmonter le problème souvent évoqué de pénurie mondiale de travailleurs qualifiés dans le domaine de la cybersécurité. En automatisant une grande partie de l'activité de détection et de réponse, vous pouvez réaffecter le personnel qualifié à des activités à plus forte valeur ajoutée, comme l'élaboration de règles de sécurité qui permettent de nouvelles activités commerciales accélérées ou la création de modèles d'intelligence artificielle (IA) qui étendent l'automatisation et la flexibilité de l'infrastructure de sécurité. L'architecture SASE fait un meilleur usage des membres de l'équipe. Il est plus adaptable que tout autre framework de sécurité d'entreprise.

Gestion de la simplicité

L'erreur humaine est l'une des principales causes de la fréquence croissante des incidents de sécurité. Cela reflète en partie la complexité à laquelle les analystes de sécurité sont confrontés, qui résulte directement de l'utilisation des systèmes de sécurité et réseau existants pour des tâches pour lesquelles ils n'ont jamais été conçus. Ces systèmes sont

aux prises quotidiennement avec un monstre moderne qui a surgi sous la forme de dizaines d'applications de surveillance qui ne parlent pas le même langage entre elles ni avec les personnes qui les administrent. Le SASE fournit un plan clair pour permettre aux nombreux services de sécurité de travailler ensemble d'une manière compréhensible.

Briser les mythes sur le SASE

ATTENTION

Ce n'est probablement pas le premier livre *pour les nuls* que vous lisez sur le SASE, et ce ne sera probablement pas le dernier, mais notre travail consiste à faire de cet ouvrage le meilleur qui soit ! Blague à part, comme pour toute technologie ou tendance émergente, le SASE fait l'objet de désinformation. De même que l'ajout d'un *i* devant le nom d'un produit ne donne pas automatiquement de l'élégance à son design et que l'ajout d'un *e* ne confère pas de la puissance et de l'efficacité, le sigle SASE fait déjà l'objet d'une grande appropriation, d'un marketing excessif et d'une mauvaise interprétation. Voici plusieurs mythes courants à son sujet.

Mythe : le SASE peut être pris en charge par les technologies existantes

L'infrastructure de sécurité réseau d'aujourd'hui est le fruit d'années (dans certains cas, de décennies) de développement et d'efforts commerciaux. Or, aucun correctif, aucune modification et aucune vente incitative ne transforment par magie les anciennes appliances en solutions de sécurité cloud. Le cloud exige une nouvelle approche.

Mythe : le SASE peut être conçu sur la base d'une SWG ordinaire

Auparavant, les passerelles web sécurisées (SWG) étaient dédiées au contrôle d'accès et à la défense contre les menaces web. Le SASE a un mandat beaucoup plus large qui inclut également les applications, les services cloud, la protection des données et la prévention des pertes de données. (Le chapitre 2 examine en détail comment les services de passerelles web sécurisées de nouvelle génération (NG-SWG) répondent à ces besoins plus larges).

Mythe : le SASE vous permet de conserver votre architecture réseau

Le SASE ne peut être efficace que si ses règles et leur application se situent à la périphérie, à proximité du lieu de rencontre de vos utilisateurs, appareils et applications. C'est cette proximité qui confère au

SASE ses caractéristiques de sécurité dynamique et qui fournit les performances et la fiabilité dont les utilisateurs ont besoin pour être plus productifs (et moins frustrés !).

Mythe : le SASE n'a pas besoin de voir tout le trafic de votre réseau

Le SASE est efficace précisément parce qu'il s'agit d'une approche globale de la sécurité. Sa puissance, sa simplicité et son impact sont favorisés par sa capacité à développer le contexte des utilisateurs, des données et des applications, y compris les API sous-jacentes. Le SASE prospère grâce à la visibilité. Ce contexte enrichi est précisément ce qui rend le SASE si efficace dans un paysage qui offre beaucoup moins de points de contrôle que l'ancien datacenter.

Mythe : le SASE complique encore les choses

La complexité est le fléau de votre existence et de celle de tous les responsables de la sécurité ou des réseaux. Elle est à l'origine de la majorité des échecs de la sécurité qui font la une des journaux. Le SASE exige que chaque élément de votre sécurité réseau fonctionne en harmonie. La sécurité réseau bricolée au coup par coup ne pourra jamais répondre à la vision du SASE pour une architecture de sécurité unique et intégrée dans le cloud, dans laquelle les règles et leur application sont parfaitement orchestrées et adaptables à l'évolution rapide des besoins.

Mythe : le SASE doit commencer par le réseau en utilisant le SD-WAN

En tant qu'avancée dans la technologie des réseaux, le Software-Defined Wide Area Network (SD-WAN) peut considérablement simplifier la gestion et l'exploitation d'un réseau étendu (WAN) et constituer une option utile (et plus rentable) par rapport aux technologies de connectivité traditionnelles comme le MPLS (Multiprotocol Label Switching). L'utilité du SD-WAN ne doit pas être écartée, pas plus que sa pertinence en tant qu'élément constitutif du SASE ne doit être ignorée. Cependant, de nombreux fournisseurs qui se concentrent sur le SD-WAN ont déjà fait un saut marketing en disant que « le SD-WAN est le bon moyen d'atteindre les objectifs du SASE », ce qui est au mieux intellectuellement malhonnête. Le SD-WAN et les pare-feux, d'ailleurs, ne sont pas la seule voie d'accès au SASE, ni les éléments de base les plus importants.

Mythe : le SASE n'a pas besoin d'un nouvel écosystème de fournisseurs

Il est pratiquement impossible pour les entreprises de se débarrasser complètement de leur passé : anciens produits, préjugés, croyances et investissements. Les entreprises qui ont l'habitude d'acquérir d'autres entreprises et technologies, et qui ont constitué de grands répertoires de connaissances institutionnelles qu'elles considèrent comme des actifs importants, ont du mal à se libérer de ces fardeaux. Le SASE est une nouvelle approche en matière de réseau et de sécurité. Vous ne pourrez pas faire face à l'avenir si vous (ou vos fournisseurs) essayez d'adapter les solutions d'hier aux besoins de demain.

DANS CE CHAPITRE

- Comprendre ce dont votre sécurité a besoin pour devenir cloud-native
- Identifier comment le SASE crée une sécurité adaptée au cloud
- Comprendre pourquoi la NG-SWG est un élément important dans le processus de mise en place d'une véritable architecture SASE
- Voir la NG-SWG en action

Chapitre 2
Reconnaître l'importance d'une NG-SWG (Next-Generation Secure Web Gateway)

Une grande partie de la stratégie de sécurité se concentrait encore récemment sur les menaces du web. Cela est logique. Avant l'adoption des services cloud, le trafic web et les liens web dans les emails étaient la principale source de menaces numériques. Les tactiques des services de sécurité, ainsi que les appliances largement utilisées comme les SWG (Secure Web Gateways), les filtres web et les appareils proxys que l'on trouve couramment sur les réseaux d'entreprise, étaient toutes adaptées à la fréquence du web.

Cette approche était également logique à l'époque où la plupart des employés travaillaient dans des bureaux et se connectaient aux ressources et à l'Internet en utilisant les réseaux de l'entreprise. Or, aujourd'hui, lorsque vos utilisateurs sont « au travail », ils sont souvent à distance ou mobiles. Ils se déplacent en utilisant différents réseaux et accomplissent leurs tâches via le cloud. Ils font appel à un

large éventail d'appareils lorsqu'ils travaillent à domicile, passent du temps productif dans leur café préféré, rendent visite à des clients et partent en déplacement. Tout cela crée une main-d'œuvre dynamique qui se connecte aux réseaux, aux applications et aux données distribués partout, tout le temps.

L'ère du cloud exige clairement une sécurité renforcée. Mais si vous avez déjà fait la queue dans un aéroport, vous savez qu'un renforcement de la sécurité n'est pas toujours synonyme d'une meilleure sécurité, et qu'il ne garantit pas une expérience utilisateur optimale. À l'aéroport, le programme TSA PreCheck et les programmes pour voyageurs dignes de confiance aident les passagers à atteindre rapidement leur porte d'embarquement. Des aspects importants des procédures de sécurité à l'aéroport contournent les agents de sécurité et autres goulets d'étranglement grâce à un processus de contrôle qui commence avant que le passager n'arrive à l'aéroport. L'objectif est d'améliorer l'expérience des passagers et de garantir une sécurité fiable et une plus grande efficacité à l'ensemble du système.

Une SWG de nouvelle génération (NG-SWG) est une étape importante vers la création d'une architecture SASE. Elle est de plus en plus souvent considérée comme la première étape, car elle permet d'avancer et de gagner en maturité sur la voie du SASE très rapidement.

Remplacer progressivement l'ancienne structure

Suivant le même modèle que l'industrie du voyage a adopté pour les voyageurs fréquents, le secteur de la sécurité a dû réexaminer comment et où assurer une sécurité renforcée. Les appliances des anciennes solutions de sécurité étaient conçues pour protéger les réseaux et les datacenters, et non pas les applications cloud. Elles n'ont pas non plus été conçues pour offrir la flexibilité et la réactivité que les utilisateurs attendent d'une expérience cloud.

Cette inadéquation — qui consiste à essayer d'utiliser d'anciennes appliances pour obtenir de nouveaux résultats — a conduit à des configurations de sécurité exigeantes et excessivement complexes qui se traduisent par des utilisateurs frustrés, une perte de productivité, des erreurs lourdes et des réponses lentes aux violations de la sécurité. Les outils de la génération précédente ne s'adaptent pas à la nature changeante du travail dans le cloud.

Voici un exemple de la façon dont ce décalage affecte la sécurité et qui illustre pourquoi le SASE est essentiel aujourd'hui : selon l'ancienne approche, les systèmes de sécurité vérifient lorsque le navigateur de

l'utilisateur établit des connexions avec les serveurs web. L'analyse de sécurité ne va pas au-delà de la vérification d'une liste pour déterminer si une URL est légitime ou si elle représente une menace. (Le chapitre 1 décrit cela comme une défense de zone).

Cela constitue un gros problème pour quiconque sécurise le cloud pour son entreprise. L'un des problèmes de sécurité qui se posent avec le plus d'acuité est celui des violations qui se produisent *à l'intérieur* de ces connexions approuvées (c'est-à-dire *après que vous avez* donné votre accord à une URL). Les hackers présentent des formulaires apparemment légitimes pour collecter des informations au sein d'une application SaaS (Software as a Service) ou d'un service cloud compromis, afin de tromper les utilisateurs pour les inciter à communiquer des données et des identifiants de connexion précieux. Parfois, les employés, dans une hâte bien compréhensible de faire les choses rapidement, coupent, copient, collent, partagent et déplacent des données sensibles à des endroits déconseillés par votre organisation. Une défense de zone ne fournit plus une protection adéquate dans un tel environnement.

La rapide montée en importance des services cloud pour les entreprises et le nombre croissant de télétravailleurs vous obligent à développer et à adopter de nouvelles approches, notamment le SASE. Votre entreprise dépendante du cloud a besoin d'une sécurité capable de s'adapter aux permutations presque infinies de l'emplacement, de l'appareil et de l'identité de l'utilisateur. L'objectif est de permettre aux utilisateurs, rapidement et en toute sécurité, d'être hautement productifs sur les applications qu'ils utilisent pour faire leur travail.

Le besoin d'une visibilité étendue

Quittons l'aéroport et prenons l'autoroute. Cette approche modulée par le web agit comme un agent de la circulation qui se tient à l'intersection où votre réseau rencontre le monde extérieur. L'agent vigilant garde un œil sur les véhicules qui passent, empêchant les conducteurs de tourner à contresens et à l'affût des véhicules suspects.

Mais dans un univers dominé par le cloud, l'agent est confronté à deux problèmes importants :

- À moins que l'agent n'ait reçu l'ordre de guetter un véhicule spécifique ou qu'un conducteur ait de toute évidence un comportement répréhensible, il ne dispose pas de beaucoup d'informations pour agir.
- Les systèmes de cybersécurité antérieurs au cloud ne regardent qu'une seule voie de trafic : le trafic web. Ces systèmes ne peuvent pas voir les nouvelles voies des SaaS, des services basés sur le cloud et des applications personnalisées — ces voies mêmes qui sont

utilisées par les cybercriminels sachant qu'elles ne sont probablement pas inspectées. L'agent ne peut pas voir les voitures et les camions qui défilent dans ces nouvelles voies, des véhicules qui pourraient cacher un trésor de diamants volés ou, en l'occurrence, vos précieuses données.

RAPPEL

Une véritable visibilité signifie avoir la possibilité de voir jusqu'à des couches fines d'activité et d'interaction entre les utilisateurs, les données et les applications. Vous devez savoir ce que vos utilisateurs font dans ces applications, en permanence. Votre utilisateur essaie-t-il de coller des données sensibles dans l'application SaaS ? Est-il sur le point d'exposer votre fichier de paie à un service public cloud ? Vos systèmes de sécurité ont besoin de savoir ce qu'il se passe.

Au-delà de la visibilité : une vaste collecte de données pour un contexte enrichi

À l'ère du cloud, la visibilité à elle seule ne suffit pas. Vous pouvez avoir une photo de la plus haute résolution possible et ne pas voir les plus petits détails de ce qu'elle représente si vous ne savez pas comment et où regarder, ou ce que vous avez devant vous. Les équipes de sécurité ont besoin de ces informations pour répondre à des questions comme celles-ci :

- Qui est l'utilisateur ?
- Quel appareil utilise-t-il ?
- Sur quel réseau se trouve l'utilisateur ?
- Quelles sont les applications auxquelles il accède ?
- Que peut-on savoir sur chaque application et son comportement ?
- Quelles sont les données auxquelles l'utilisateur accède ?
- Ses comportements actuels et passés sont-ils cohérents ?

Nous faisons référence aux détails de l'image en tant que *contexte*, qui est l'un des concepts les plus importants de l'accès au cloud. C'est ce contexte qui permet de définir et d'appliquer des règles de sécurité capables de limiter ce qui se passe, le cas échéant, dans les actions et les applications en temps réel. (Voir le chapitre 4 pour en savoir plus sur le contexte et les stratégies).

RAPPEL

Les exigences d'une sécurité efficace à l'ère du cloud sont les suivantes :

- Minimiser la complexité de votre architecture de sécurité pour faciliter le travail des utilisateurs et de l'équipe de sécurité

- Fournir aux utilisateurs, où qu'ils soient, des interactions rapides et réactives avec leurs applications afin qu'ils puissent profiter pleinement des avantages du cloud
- Gérer en permanence les risques pour vos activités en étant capable de voir facilement et de traiter rapidement les activités potentiellement risquées impliquant les données et les utilisateurs de l'entreprise

Une architecture SASE correctement mise en œuvre peut répondre à toutes ces exigences.

Le SASE : conçu pour le cloud

Vous ne pouvez pas vous contenter de renommer ou de réaffecter la technologie d'hier et penser qu'elle peut gérer les besoins actuels en matière de sécurité dans le cloud, sans parler des besoins futurs. Les anciennes appliances ne sont pas seulement freinées par le fait qu'elles sont coincées dans votre datacenter. Le cloud fonctionne également à une échelle et une vitesse totalement différentes. Les services de sécurité doivent être conçus pour fonctionner à la même vitesse et à la même échelle.

Ce qui fait du SASE un cadre de sécurité si attrayant, c'est que, tout comme le cloud, il rend le travail plus facile et plus flexible.

Le fait d'être conçu pour le cloud signifie que toutes les exigences stratégiques du SASE doivent être intégrées dès la conception de l'architecture. Pour remplir sa mission, et ce, à grande échelle, une véritable architecture SASE nécessite que chaque service impliqué dans la sécurité s'exécute de façon coordonnée, dans le cadre d'une action continue et rapide. Toutes vos vérifications et inspections doivent se faire « sur place », où que ce soit. Le trafic d'un utilisateur n'a pas besoin de revenir vers un goulet de sécurité (votre datacenter !) pour chaque interaction. En rapprochant la sécurité de l'utilisateur et des points d'accès, chaque interaction est à la fois plus sûre et plus efficace. Votre sécurité peut alors relever le défi du cloud. Pour en revenir à la métaphore de l'autoroute, avec le SASE, l'agent peut enfin voir toutes les voies de circulation.

Permettre une véritable sécurité dans le cloud

Le SASE a deux missions essentielles :

- **Fournir un *réseau périphérique mondial* qui permet à vos utilisateurs d'accéder aux services cloud, où qu'ils se trouvent :** Ce réseau périphérique mondial authentifie les utilisateurs, puis optimise leurs connexions aux applications SaaS, à votre datacenter et à d'autres services.

- **Fournir des services de sécurité sur l'ensemble du réseau périphérique mondial afin qu'ils soient proches des utilisateurs :** Ainsi, les utilisateurs et les organisations peuvent toujours compter sur ce réseau de sécurité pour effectuer leur travail en toute sécurité. Cette configuration permet également d'appliquer des politiques de sécurité et de dicter les interactions en ligne des utilisateurs en fonction de leur identité et de l'endroit où ils se trouvent, et ce, tout en optimisant la sécurité, la fiabilité et les performances de ces activités.


RAPPEL

Une architecture SASE correctement implémentée est efficace, car elle reconnaît que les applications et les workloads sont désormais gérées dans le cloud, et que les services de sécurité doivent donc suivre. Pour vos utilisateurs, cela signifie qu'ils n'auront pas à faire des « pirouettes » pour pouvoir utiliser une application. Lorsqu'ils se rendront dans un café, avoir accès à ce dont ils ont besoin sera aussi simple que de commander un latte. Pour vous, le professionnel de la sécurité, le fait de disposer d'un contexte et de services de sécurité intégrés et partagés permet de créer des politiques performantes qui peuvent être appliquées automatiquement et de manière appropriée en fonction des personnes qui ont besoin d'un accès, de ce à quoi elles essaient d'accéder et de l'emplacement où se trouvent tous les éléments de l'interaction. Dans un monde digital qui a quitté les limites restrictives du datacenter pour les possibilités très ouvertes du cloud, le modèle SASE est la *seule* architecture réseau et de sécurité qui ait du sens.

Qu'en est-il du datacenter ?

Le datacenter a encore un rôle à jouer dans l'informatique d'entreprise dans un avenir proche. Les applications volumineuses comme les progiciels de gestion intégrés (ERP) ont été conçues pour durer des dizaines d'années, de sorte que les applications du cloud privé coexisteront sans doute longtemps avec les SaaS et les applications du cloud public. Plus généralement, les organisations ont beaucoup investi pendant de nombreuses années pour créer et entretenir leurs datacenters d'entreprise. Il peut être difficile de mettre fin à cet élan. Soyez donc patient.


RAPPEL

Lorsque vous considérez le datacenter comme l'un des nombreux endroits où vos utilisateurs se rendent pour faire leur travail, le fait d'y faire transiter tout votre trafic cloud entrant commence à perdre son sens. Obliger le trafic d'un utilisateur à faire constamment un détour par le réseau privé de votre organisation pour passer ensuite par une succession de boîtes noires de sécurité distinctes (un processus que les spécialistes de la sécurité appellent *hairpinning* ou *backhauling*) est un processus lourd et inefficace. Après tout, vous n'envisageriez pas de conduire de Los Angeles à San Francisco en passant par Le Caire, à

moins d'avoir beaucoup de temps libre (et un bateau). La même logique s'applique pour relier vos utilisateurs à leurs applications SaaS.

CONSEIL

Le SASE ne concerne pas seulement les applications SaaS. Il peut et doit être utilisé pour fournir un accès à toutes vos applications et les protéger, y compris celles qui se trouvent dans le datacenter, que l'utilisateur soit on-premise ou off-premise.

Les services qu'il faut pour chaque scénario

La flexibilité est l'un des grands avantages des services cloud. Mais il ne suffit pas de coller des mots comme *cloud* ou *SASE* sur un produit pour y parvenir. La flexibilité doit être intégrée intentionnellement dans l'implémentation d'une véritable architecture SASE. Étant donné que le contexte dans le cloud change constamment, différentes technologies et différents services devront travailler ensemble sur une base ad hoc et être appliqués au fur et à mesure que les scénarios changent et évoluent. S'il est correctement implémenté, le SASE applique tous les services de sécurité nécessaires à la stratégie de sécurité pour n'importe quelle connexion, tout en donnant toujours la priorité aux objectifs suivants :

- Adaptation à une main-d'œuvre décentralisée
- Optimisation des niveaux de service en fonction de l'évolution du contexte
- Garder les services de sécurité aussi proches que possible des utilisateurs à tout moment
- Fournir les services de sécurité nécessaires pour fonctionner en hyperscale tout en garantissant les performances requises par les flux de travail des entreprises modernes

La question que nous devons maintenant nous poser est la suivante : comment faire évoluer votre organisation vers un SASE efficace ? Dans les sections suivantes, nous examinons certaines exigences clés, dont une importante, la NG-SWG.

Besoin d'un réseau périphérique mondial

Si l'on regarde à travers le prisme des anciennes architectures de sécurité, l'idée même de sécuriser le cloud pour les entreprises semble être contradictoire. D'un côté, vous avez des utilisateurs qui comptent sur vous pour leur fournir un accès rapide à leurs applications et à leurs données, depuis n'importe où, avec un minimum de perturbations causées par des barrages de sécurité. Cela va quasiment à l'encontre de l'attente selon laquelle vous devez également assurer à vos utilisateurs et à votre entreprise une sécurité et une protection des données maximales.

Le *hairpinning* du trafic dans votre datacenter n'était pas un problème important lorsque 85 % des utilisateurs travaillaient dans les locaux de l'entreprise. Dans le monde créé par la pandémie de COVID-19, de plus en plus de travailleurs ont goûté au télétravail et 74 % d'entre eux souhaiteraient désormais travailler à domicile au moins deux jours par semaine, selon une enquête de PwC. Pour les utilisateurs distants, le *hairpinning* introduit de la latence et des obstacles qui entravent une expérience utilisateur productive. Le télétravail étant probablement la nouvelle norme, il est impératif que la sécurité se déplace vers le cloud où elle peut le mieux suivre ces utilisateurs et assurer la protection des données sans dégrader l'expérience utilisateur.

Ce dernier point est important, car les utilisateurs frustrés qui veulent un accès rapide éviteront de se connecter à votre réseau privé virtuel (VPN), ce qu'ils font déjà depuis des années. Dans ce cas, vos utilisateurs et vos données ne sont pas du tout protégés, et votre équipe chargée de la sécurité ne sait plus où donner de la tête. Un réseau périphérique mondial permet aux utilisateurs de se connecter au cloud de n'importe où sans avoir à revenir vers le datacenter pour protéger et sécuriser les données.

RAPPEL

L'accès à un réseau périphérique mondial constitue un avantage certain pour votre personnel mobile. Le réseau périphérique mondial de Netskope fournit des points d'accès dans plus de 40 régions du monde où les fonctions de sécurité sont hébergées et exécutées. C'est ce qui permet de maintenir la sécurité à proximité de l'utilisateur à tout moment et de fournir une inspection à passage unique du trafic ou « single-pass » (voir « Inspection single-pass », ci-après dans ce chapitre, pour en savoir plus. Pour l'instant, disons simplement « inspection rapide »). Ensemble, ces points d'accès contribuent à offrir une expérience utilisateur fluide, rapide et sécurisée.

L'une des différences fondamentales entre le SASE et la sécurité traditionnelle réside dans la manière dont la sécurité est appliquée et le lieu où elle est appliquée. Dans une architecture de sécurité SASE, lorsqu'un utilisateur souhaite se connecter à Internet — que ce soit pour utiliser une application SaaS, surfer sur le web ou publier sur un réseau social — il se connecte d'abord à un point d'accès sur le réseau périphérique mondial. Chaque point d'accès intègre les capacités de calcul nécessaires pour alimenter les services de sécurité. Grâce à cette répartition, les utilisateurs ne sont pas confrontés aux compromis en matière de performances ou aux problèmes de sécurité complexes et à plusieurs niveaux qu'ils rencontraient lorsque tout passait par le datacenter de l'entreprise.

Comprendre le lien entre NG-SWG et SASE

La forme idéale et complète du SASE est une nouvelle architecture de sécurité dans laquelle le fonctionnement de tous vos services de sécurité est parfaitement coordonné. Cela apparaît comme un projet de grande envergure ? C'est bien le cas. Mais vous n'êtes pas obligé d'arriver à ce résultat tout de suite. C'est en faisant les bons premiers pas que vous créerez une base solide pour tout ce qui suivra. Une première étape clé consiste à implémenter une NG-SWG. C'est ce qui fait vraiment la différence entre un « semblant de SASE » et un SASE correctement exécuté. Catalyseur qui permet de créer la sécurité dans le cloud, c'est la NG-SWG qui rend le SASE possible.

La meilleure façon d'implémenter le SASE est d'utiliser une architecture de microservices. En termes simples, les *microservices* sont un moyen de créer un système à partir de nombreux modules de services petits et distincts. Lorsqu'ils sont bien conçus, ces modules partagent une base de code commune et travaillent en synergie pour comprendre le langage natif du cloud.

Tous ces services doivent être orchestrés pour fonctionner ensemble afin d'appliquer vos stratégies de sécurité en fonction du contenu et du contexte. La NG-SWG fait office de contrôleur aérien pour une implémentation du SASE. Quels que soient le lieu et le moment où l'utilisateur accède aux données, la NG-SWG coordonne les services afin qu'ils agissent de concert pour appliquer les stratégies de sécurité dans l'ensemble de l'environnement informatique.

En une seule séquence rapide, la NG-SWG applique tous les services de sécurité partagés nécessaires à l'application de la sécurité basée sur des stratégies à chaque connexion, sur la base d'une compréhension enrichie des utilisateurs, des données, des applications et du trafic sur votre réseau.

La NG-SWG vous permet également de mettre hors service les appliances les moins performantes, réduisant ainsi la complexité de votre infrastructure de sécurité sans renoncer aux caractéristiques de leurs services les plus utiles. Ces services, qui font désormais partie de la NG-SWG, sont appliqués en coordination avec les nombreux nouveaux services qui collaborent pour inspecter en profondeur votre trafic SaaS et web, afin d'acquérir cette compréhension enrichie et d'appliquer des stratégies de sécurité basées sur le contexte.

ATTENTION

Une plateforme de cloud public générique comme Amazon Web Services (AWS) ou Google Cloud n'est pas un SASE, ni même compatible avec le SASE, à elle seule. Les solutions de cloud public sont optimisées pour fournir des applications, l'architecture de cloud public étant conçue comme une destination plutôt que comme un hub de services de sécurité par lequel le trafic passe pour aller ailleurs. Le SASE a des exigences de calcul et de performance uniques qui permettent de prendre en charge une architecture basée sur des microservices conçue pour les charges de travail de sécurité.

Comparaison des SWG et des NG-SWG

Les SWG sont parfois appelées passerelles web sécurisées ou proxys web ou filtres web (ou autrement). Elles existent sous une forme ou une autre depuis au moins les années 90 et ont été conçues à une époque très différente.

Qu'est-ce qui différencie les NG-SWG des SWG traditionnelles et d'autres produits similaires que vous connaissez peut-être ? La réponse la plus simple est que la SWG traditionnelle ne gère que le trafic web et ne fournit que des contrôles d'autorisation ou de refus. Elle a été conçue à une époque où l'Internet se résumait à des sites web et à des communications HTTP/S (Hypertext Transfer Protocol/Secure). En d'autres termes, il s'agissait de décider si « oui, vous pouviez accéder à ce site web » ou « non, vous ne pouviez absolument pas accéder à *ce* site web ».

La NG-SWG, en revanche, est le parapluie organisationnel sous lequel résident tous les services web et autres, tout en créant une sécurité expansive cloud avec des points de contrôle à proximité de l'utilisateur (le réseau périphérique mondial mentionné plus haut) où une large gamme de services de sécurité sont orchestrés. La NG-SWG exécute et améliore toutes les fonctions de base du trafic web dans les anciennes SWG et les appliances similaires et ajoute de nouvelles fonctions de sécurité importantes. En particulier, la NG-SWG procède à une inspection approfondie du trafic cloud et web, en cherchant à voir ce qui se passe dans les interactions, en appliquant la protection des données et contre les menaces, et en développant une compréhension du contenu et du contexte pour appliquer des contrôles de stratégie granulaires.

Avec la NG-SWG de votre SASE, l'agent de circulation ou le contrôleur peut voir toutes les voies de circulation, savoir ce qui se passe à l'intérieur des véhicules et faire respecter les règles (voir le tableau 2-1).

TABLEAU 2-1 **Comment Netskope répond aux exigences du SASE**

Exigence du SASE	Netskope NG-SWG
Cloud-native avec une architecture single-pass pour l'inspection du trafic chiffré	Réside entièrement dans le cloud en utilisant l'architecture cloud-native avec la capacité de décoder et de comprendre les applications et les services cloud pour le contexte des données. L'architecture single-pass de Netskope assure l'inspection avancée des données et des menaces du trafic chiffré (prise en charge de TLS1.3 sans négociation descendante de la connexion) à la vitesse filaire dans chaque datacenter NewEdge pour tous les services (SWG, CASB [Cloud Access Security Broker], protection avancée contre la perte de données [DLP], sandboxing, analyse par Machine Learning [ML], pare-feu « as a service » [FWaaS], isolation du navigateur à distance [RBI], etc.)
Points de présence, avec des accords de niveau de service (SLA) pour une faible latence et une haute disponibilité	Netskope NewEdge Network, un cloud privé de sécurité hautes performances, héberge des services de sécurité et fournit de nombreux points d'accès dans le monde entier. Offrant une latence de quelques millisecondes pour la meilleure expérience possible, NewEdge est soutenu par un accord de niveau de service (SLA) à 99,999 % de disponibilité en mode inline, plus un portail de confiance indiquant le statut de service/datacenter en temps réel (`https://trust.netskope.com`).
« Security-as-a-service » via un control plane dédié aux politiques de sécurité.	Une unique plateforme cloud et un moteur de règle qui s'exécute sur un management plane séparé du data plane utilisé pour le contrôle du trafic. Pour faciliter l'administration, une console unique permet de gérer et d'ajouter tous les services de sécurité du SASE, qui sont déployés via un agent unique pour un accès et une expérience utilisateur simplifiés sur tous les sites.
Inspection du trafic via le « forward proxy » de la NG-SWG pour cinq types de trafic utilisateur	Analyse toutes les voies du trafic utilisateur sur le Web, les SaaS gérés, les applications en Shadow IT, les services cloud publics et les applications personnalisées dans le cloud public ou le datacenter, contrairement aux anciennes SWG qui analysent uniquement le trafic web. Des stratégies d'inspection de sécurité cohérentes sont appliquées à toutes les méthodes d'accès.
Visibilité et contrôle des données sensibles et DLP dans le cloud	Visibilité inégalée sur les services web, SaaS, Shadow IT, cloud public et les applications personnalisées dans le cloud public pour les mouvements de données sensibles. Protège les données en mouvement pour cinq types de trafic utilisateur plus la DLP de la messagerie pour le trafic sortant Microsoft Office 365 (M365) et le SMTP (Gmail Simple Mail Transfer Protocol). Le principal objectif de cette fonctionnalité est d'analyser le mouvement de données entre les applications personnelles et professionnelles et les instances d'applications, ainsi que les anomalies de mouvement de données.

(suite)

TABLEAU 2-1 *(suite)*

Exigence du SASE	Netskope NG-SWG
Protection contre les menaces avancées (ATP) et analyse comportementale des utilisateurs et des entités (UEBA)	Offre une protection contre les malwares, le phishing et les documents malveillants basés sur le web et le cloud, grâce à un antimalware en mode inline, une analyse de préexécution, un sandboxing, une analyse par Machine Learning et l'UEBA pour les anomalies de comportement et l'évaluation des risques pour l'utilisateur, avec des analyses en temps réel et une visualisation du tableau de bord sur tous les utilisateurs/applications concernant les données, les menaces et l'activité.
Pare-feu cloud	Permet de contrôler les pare-feux cloud sortants pour les utilisateurs itinérants et les sites distants sur tous les ports et protocoles.
RBI	Le pixel RBI ciblé affiche les sites web non catégorisés et risqués afin d'offrir un accès sécurisé aux utilisateurs. Il bloque également les chargements et téléchargements de fichiers, les entrées de formulaire des attaques de phishing, et le copier-coller du presse-papiers.
Politique de sécurité réseau Zero Trust	Les contrôles de sécurité Zero Trust sont appliqués en commençant par l'accès utilisateur (accès au réseau Zero Trust [ZTNA], gestion des identités et des accès [IAM]) pour capturer les informations sur les risques et le contexte de l'utilisateur, le type d'appareil, l'application, l'instance d'application, l'évaluation des risques de l'application, la catégorie, l'activité, le contenu et l'action en vue d'appliquer des contrôles de stratégie conditionnels et contextuels basés sur les risques. Au fur et à mesure que le comportement de l'utilisateur et les anomalies sont surveillés, des actions de stratégie adaptatives sont dynamiquement appliquées selon les principes Zero Trust, notamment des tests d'authentification plus poussés, la limitation de l'accès aux activités, du mouvement des données ou l'arrêt complet de l'accès aux applications de l'utilisateur.
Création de stratégies adaptatives en fonction du contexte et application cohérente	Fournit un encadrement en temps réel, une authentification renforcée et des stratégies adaptatives basées sur les risques liés aux applications, aux utilisateurs et au contexte des données. L'application en temps réel est cohérente pour tous les utilisateurs, les sites distants et les autres sites du réseau périphérique.
IAM	S'intègre aux systèmes IAM et de fournisseurs d'identité qui gèrent et vérifient l'identité numérique des utilisateurs et des groupes.
Protection des points de terminaison	Permet le partage bidirectionnel automatisé des indicateurs de compromission (IOC), ainsi que l'accès conditionnel avec activation de la protection des points de terminaison et la possibilité de partager des métadonnées enrichies pour les enquêtes.
Gestion des événements et des informations de sécurité (SIEM) et centre des opérations de sécurité (SOC)	Fournit le partage des indicateurs de compromission (IOC) et des métadonnées enrichies pour travailler de manière transparente avec les points de gestion et les tableaux de bord utilisés par le personnel de sécurité pour enquêter sur les alertes et les incidents.

Exigence du SASE	Netskope NG-SWG
Analyse et visualisation en temps réel	Fournit des métadonnées cloud pour une visualisation et une analyse en temps réel des mouvements de données, des menaces, des utilisateurs et des applications dans des tableaux de bord personnalisables dynamiques destinés à l'équipe de direction, au conseil d'administration, et aux équipes de gestion de la sécurité et des risques.

Un peu de SASE par rapport à un modèle SASE correctement implémenté

Avec la NG-SWG, vous n'avez plus besoin de configurer des centaines ou des milliers de minuscules règles, détaillées mais compliquées, séparément pour chacune de vos solutions et appliances de sécurité, dont chacune ne gère qu'une petite partie du trafic dans votre datacenter. Dans les meilleures solutions SASE utilisant une NG-SWG, vous vous concentrez sur la création de stratégies générales qui décrivent les résultats que vous souhaitez obtenir pour *tout* le trafic. La NG-SWG indique ensuite aux différents services de sécurité ce qu'ils doivent faire pour obtenir ces résultats sur votre trafic web, vos applications SaaS gérées ou non gérées (Shadow IT), vos services de cloud public et vos applications personnalisées hébergées dans le cloud public. L'application de la stratégie peut même inclure des fonctionnalités avancées comme l'accompagnement de l'utilisateur et des actions basées sur le risque pour permettre des réponses nuancées et appropriées. Vous définissez les choses que vous souhaitez voir se produire dans l'architecture, et la NG-SWG coordonne les services pour y parvenir.

JARGON TECHNIQUE

Comment la NG-SWG crée-t-elle les bases contextuelles pour une implémentation correcte du SASE ? Le tableau 2-1 (plus haut dans ce chapitre) décrit les services et les fonctionnalités fournis par une NG-SWG dans une architecture SASE. Il présente également les autres services qui permettent de compléter la solution SASE lorsqu'ils sont connectés à Netskope NG-SWG.

Examen du fonctionnement de la NG-SWG

La section précédente décrit ce que les NG-SWG fournissent dans le cadre de l'architecture plus large du SASE. Cette section examine comment la NG-SWG met tout cela en action.

RAPPEL

Bien que la description suivante soit organisée en sections, n'oubliez pas que la sécurité avec la NG-SWG ne correspond pas à une chaîne d'appliances séparées ou une séquence linéaire d'opérations comme dans un datacenter.

Inspection single-pass

Lorsque l'appareil d'un utilisateur est connecté à un point d'accès sur le réseau mondial EDGE, tout le trafic de l'utilisateur est soumis à une inspection single-pass. *Single-pass* signifie exactement ce que vous pensez : tous les services de sécurité nécessaires à l'application de la stratégie forment un entonnoir continu par lequel passe le trafic. Le trafic entre l'utilisateur et la destination passe par cet entonnoir unique une fois, en temps réel. Ce processus est différent de celui des anciennes solutions de trafic intégrées au cloud et des appliances SWG réservées au web, qui revenaient à avoir une série d'entonnoirs indépendants par lesquels tout devait passer.

L'inspection single-pass de la NG-SWG s'applique au contenu web, aux applications SaaS gérées par votre organisation, à toute application SaaS en Shadow IT ou non gérée qu'un utilisateur tente d'utiliser, aux services de cloud public et à toute application personnalisée dans le cloud public déployée par votre organisation. Le trafic web et cloud passe par ce système unique, qui regroupe et coordonne tous les services de sécurité en une seule plateforme cohérente, puis les améliore pour donner vie à une architecture SASE correctement implémentée.

Le trafic est filtré, en un seul passage, par étapes. Les problèmes les plus évidents sont éliminés en premier, laissant une quantité de plus en plus faible de trafic à soumettre à une analyse plus détaillée (voir le chapitre 4 pour plus de détails sur ces étapes).

Plus le contexte est riche, plus la sécurité est forte

Le contexte est essentiel à la sécurité active, profonde et agile qu'offre une architecture SASE correctement implémentée. Dès qu'un utilisateur se connecte à un point d'accès, les services de la NG-SWG dans le cadre de la sécurité du cloud élaborent une image contextuelle disponible pour tous les services. Cette image est utilisée pour dicter la manière dont la stratégie est appliquée. Ce contexte constitue un conglomérat massif de *métadonnées* (données qui décrivent d'autres données ou ajoutent un contexte), notamment une multitude d'informations qui identifient et reconnaissent les éléments suivants :

- L'utilisateur ou le groupe organisationnel auquel l'utilisateur appartient
- L'appareil de l'utilisateur, son emplacement et si cet appareil est géré par votre organisation
- Le site web, l'application ou la suite d'applications avec lesquels l'utilisateur travaille

- L'indice de confiance du cloud de Netskope : une évaluation du risque dérivée de plusieurs services indépendants d'évaluation de la sécurité et attribuée au site web, à l'application ou à la suite d'applications en question
- Les données demandées, générées et/ou utilisées par l'utilisateur et l'application

En outre, ce contexte est enrichi par de nombreuses sources d'informations nouvelles et variées que la NG-SWG peut exploiter pour ajouter des détails supplémentaires sur la base des éléments suivants :

- Connaissance du comportement de l'utilisateur et de toute anomalie dans ce comportement
- Inspection du contenu et des données contenues dans le trafic
- Activités réalisées par l'application, le contenu web et les services accessibles, et la nature de ces activités
- Connaissance des données dans l'environnement applicatif
- Informations stockées recueillies lors d'interactions passées

Le contexte change constamment pendant toute la durée de l'accès de l'utilisateur. Vous devez donc avoir un système qui soit souple, réactif et adapté aux variations subtiles du risque présenté par différentes combinaisons de détails contextuels. La stratégie peut décrire le résultat souhaité en matière de sécurité, mais c'est le contexte qui détermine la combinaison optimale de services et d'actions de sécurité permettant d'obtenir ce résultat, en fonction des particularités du moment. Par exemple, un utilisateur qui se comporte soudainement de façon étrange et qui accède à des fichiers qu'il ne devrait pas avoir, fait l'objet d'une *authentification renforcée, c'est-à-dire d'une* demande d'informations supplémentaires pour établir son identité. Le fait de disposer d'un vaste contexte dynamique permet d'appliquer des stratégies de sécurité granulaires et d'activer des actions de stratégie en temps réel à mesure que le contexte change. L'intelligence artificielle (IA) et le ML jouent un rôle majeur pour permettre à votre système de sécurité de passer au crible ces détails contextuels nuancés (voir le chapitre 4).

RAPPEL

La sécurité web traditionnelle était essentiellement une proposition de type « oui ou non ». La NG-SWG est une approche dynamique et continue de la sécurité qui observe en permanence le comportement et ce qui se passe dans tout le trafic web et cloud. Elle peut ainsi adapter à la volée ses décisions en matière de sécurité, une capacité essentielle pour sécuriser l'interaction des utilisateurs avec les applications et les sites web.

JARGON TECHNIQUE

Le tableau 2-2 décrit certains des services de sécurité étendus et améliorés par la NG-SWG et qui constituent la base d'une architecture SASE complète.

TABLEAU 2-2 Principaux services de sécurité fournis par la NG-SWG

Service de sécurité	Objectif du service dans une configuration traditionnelle	Comment la NG-SWG booste le service
SWG	Protection des utilisateurs contre les menaces du web et les contenus répréhensibles.	Ajoute le contexte de l'application et des données (quel utilisateur utilise l'application ou les données, où il l'utilise et pourquoi). Ajoute la protection des données (en empêchant leur modification ou leur vol). Prévient l'utilisation inappropriée des données (en empêchant que les données soient utilisées ou envoyées là où elles ne devraient pas l'être).
DLP	Protection uniquement des données stockées dans le datacenter et qui sont déplacées au-delà du pare-feu du datacenter via le web.	Protège toutes les données en mouvement, y compris les données distribuées sur le web, dans les applications SaaS, dans le cloud, dans les services cloud et dans les applications personnalisées sur le cloud public.
CASB	Surveillance et protection des applications gérées qui fournissent des interfaces de programmation d'applications (API) visibles et qui peuvent être surveillées et protégées via ces API, mais aussi en mode inline. L'accent est mis sur les données au repos et les données en mouvement, c'est-à-dire les données stockées dans l'environnement de l'application ou dans le datacenter, ainsi que celles qui transitent entre les deux. Toutes les solutions ne prennent pas en charge tous les modes.	Surveille les applications non gérées qui n'offrent pas d'API de gestion évidente, ce qui permet de surveiller et de protéger un grand nombre d'applications non gérées. Surveille les données en mouvement. Les données activement utilisées par les applications et les sites web et qui leur sont transmises peuvent donc être protégées. Offre des informations solides sur les risques liés aux applications afin de faciliter la sélection et le déploiement de SaaS.

Service de sécurité	Objectif du service dans une configuration traditionnelle	Comment la NG-SWG booste le service
Protection contre les menaces avancées (ATP)	Protection contre les menaces basées sur le web à l'aide de méthodes telles que le *sandboxing* (détonation des exécutables en toute sécurité pour détecter les intentions malveillantes et les hyperliens) et surveillance des menaces (partage d'IOC provenant de sources publiques et payantes).	Protège contre les menaces liées au cloud, notamment la diffusion de logiciels malveillants et les attaques de phishing à l'aide d'applications et de services cloud comme Microsoft Office 365 et Google Docs. Isole les applications et sites web inconnus pour interagir en toute sécurité et se protéger contre les menaces potentielles.

Application d'une stratégie single-pass

Bien entendu, même le contexte le plus détaillé n'est pas utile si les utilisateurs et les services de sécurité ne savent pas ce qu'ils sont censés faire et ne pas faire. Vous avez donc besoin de règles de base auxquelles le contexte peut être comparé.

Vous avez peut-être rédigé un ensemble de règles qui dictent le comportement du pare-feu, en vérifiant l'URL saisie par un utilisateur par rapport à des listes de sites web que vous avez décidé de bloquer. Mais la sécurité traditionnelle oblige toujours à faire des compromis entre la rapidité et la flexibilité d'une part, et la sécurité d'autre part. Entre le flux constant de nouveaux sites et les changements de personnel au fil du temps, votre liste de règles peut devenir extrêmement volumineuse et fragile. Peut-être hésitez-vous à modifier vos règles, par exemple pour permettre l'accès à un outil de vente utile, de peur d'ouvrir involontairement une nouvelle vulnérabilité.

Le SASE, s'il est bien implémenté, élimine ces compromis en proposant un nouveau modèle pour assurer une sécurité hors pair. L'application de la stratégie single-pass est le pouvoir, ou le superpouvoir, propre à SASE d'appliquer la stratégie de données ou les contrôles d'activité à l'ensemble des applications, catégories d'applications et services web. Pensez-y comme le pouvoir du contexte en action. Par exemple, si l'inspection single-pass détecte un type de données sensibles dans un formulaire web, dans un fichier ou un champ d'une application ou dans un canal Slack, l'application de la stratégie single-pass peut bloquer le contenu sur le web et/ou contrôler l'activité dans l'application (chargement) tout en autorisant l'affichage.

Grâce à un cadre de stratégie cohérent, granulaire et centralisé qui s'étend à tous vos services de sécurité, vous pouvez prendre le contrôle

et déclarer clairement vos intentions, sans vous soucier des détails de l'implémentation d'une stratégie spécifique. Cela réduit considérablement la complexité.

CONSEIL

Le SASE et la NG-SWG transforment le travail de votre équipe de sécurité. Au lieu d'écrire un code distinct et inefficace pour gérer chaque appliance, votre équipe se concentre sur l'écriture de règles efficaces et générales pour fournir des services qui ont du sens pour l'entreprise.

La NG-SWG en action

La figure 2-1 montre à quoi ressemble une NG-SWG en action du point de vue d'un seul utilisateur.

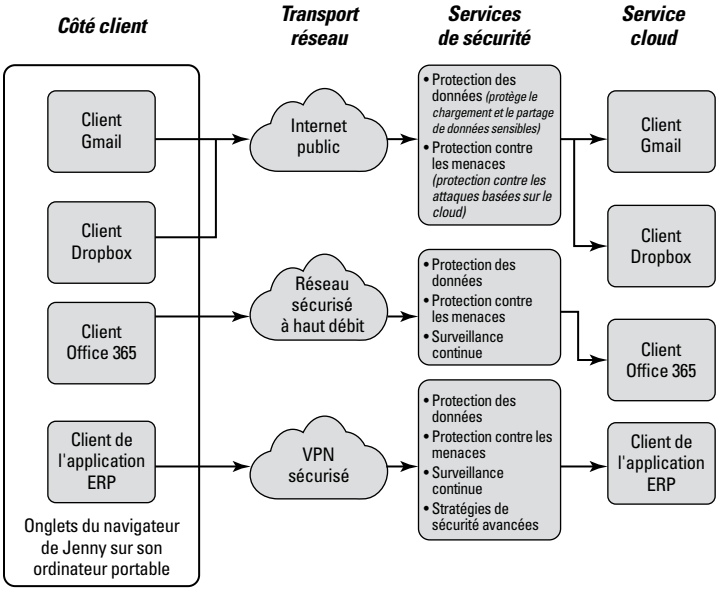

FIGURE 2-1 : NG-SWG en action pour une seule utilisatrice nommée Jenny.

Dans la figure 2-1, Jenny représente un utilisateur typique travaillant à domicile pouvant initier quatre connexions de son ordinateur portable à

- Son compte personnel Gmail
- La messagerie Microsoft Office 365 de son entreprise
- Une application de stockage cloud comme Dropbox
- Des applications stratégiques gérées par l'entreprise, comme Salesforce, ServiceNow ou Workday.

Dans ce cas, la NG-SWG traite ces interactions distinctes comme suit :

- **L'application Gmail personnelle de Jenny est routée vers l'Internet public.** La NG-SWG sécurise et analyse la connexion, assurant la protection contre les menaces et la protection des données, ce qui se traduit par une expérience utilisateur très performante.
- **Le courrier électronique Microsoft Office 365 de l'entreprise de Jenny est acheminé sur un réseau sécurisé à haut débit.** Le trafic de cette connexion est surveillé en permanence pour s'assurer que des données cruciales ne sont pas partagées.
- **La connexion à l'application de stockage cloud non gérée Dropbox est acheminée via l'Internet public.** La NG-SWG sécurise et analyse cette connexion en permanence et applique la stratégie de sécurité, permettant ainsi à Jenny de visualiser des fichiers partagés provenant de sources tierces. Toutefois, la NG-SWG bloque les transferts et applique la prévention des menaces aux téléchargements de fichiers lorsqu'une justification a été fournie par Jenny pour le téléchargement de fichiers.
- **La connexion de Jenny à l'application d'entreprise stratégique est acheminée par un VPN spécial et chiffré.** La connexion est contrôlée par plusieurs services de sécurité différents qui fournissent des couches de protection pour garantir que les données ne sont pas partagées ou utilisées de manière inappropriée. La NG-SWG applique également des stratégies pour s'assurer que l'application est utilisée correctement.

Dans cet exemple, vous pouvez voir avec un seul travailleur comment quatre connexions différentes sont protégées. Chaque connexion a un contexte distinct qui dicte l'application de politiques spécifiques et pertinentes. L'expérience utilisateur qui en résulte est excellente, et le niveau de sécurité est élevé. Jenny peut consulter son compte Gmail personnel et faire son travail sans risquer de compromettre les données de l'entreprise. Voilà la différence que la NG-SWG peut apporter.

À ce stade, il est important de noter que la NG-SWG n'est pas la *seule* solution à se démarquer dans le cadre d'une architecture SASE correctement implémentée. La NG-SWG n'est pas une solution miracle. La fonctionnalité CASB (que l'on ne trouve pas dans une SWG, mais dans une véritable NG-SWG) et l'application judicieuse des principes Zero Trust sont d'autres pièces essentielles du puzzle.

La NG-SWG est cependant primordiale. Elle peut accélérer considérablement votre parcours dans le domaine du SASE et vous permettre d'abandonner les vieilles technologies comme les anciennes SWG qui ne feront qu'entraver la réussite de votre architecture SASE.

DANS CE CHAPITRE

- **Améliorer la sécurité en connaissant mieux son personnel**
- **Examiner quelle combinaison de services renforce la sécurité**
- **Comprendre comment la confiance change lorsque les gens travaillent en dehors du réseau que vous contrôlez traditionnellement**
- **Découvrir comment booster la sécurité pour protéger les personnes dans le cloud**

Chapitre 3
Protéger les personnes

Une grande partie de la sécurité concerne les personnes. Votre objectif consiste à protéger les personnes et les choses qui comptent pour vous contre les personnes ayant de mauvaises intentions. Pour les équipes chargées de la sécurité et de la gestion du réseau des entreprises, les scénarios évidents sont ceux qui visent à protéger le personnel et les actifs numériques de l'organisation contre ceux qui pourraient leur nuire, tout en veillant à ce que les employés et les clients bénéficient d'expériences satisfaisantes et fiables.

Mais la sécurité consiste également à protéger votre personnel contre lui-même, notamment contre les faux pas, les tentations, les négligences et les erreurs de jugement qui peuvent causer un préjudice irréparable, à lui ou à votre entreprise. (Vous serez peut-être surpris d'apprendre que plus de 90 % des incidents de cybersécurité sont imputables à une erreur humaine, selon Kaspersky Lab).

Le SASE (Secure Access Service Edge), lorsqu'il est correctement conçu, fournit à votre personnel de sécurité les informations et les outils nécessaires pour relever efficacement et intelligemment ces vastes défis en aidant votre organisation sur deux fronts :

- **Protéger vos systèmes contre les personnes qui ne sont pas autorisées à y accéder :** que ces systèmes se trouvent dans votre datacenter ou dans le cloud, la même norme doit être appliquée à tout moment.

- **Lorsque des personnes sont autorisées à entrer dans vos systèmes, les empêcher de faire des choses dangereuses, intentionnellement ou non.**

Le SASE déplace la sécurité vers un environnement cloud en périphérie, en créant une structure riche en services de sécurité, qui offre une visibilité et un contrôle complets, et peut être accessible partout.

Ce chapitre examine comment un SASE bien implémenté, conçu à l'aide de la NG-SWG (Next-Generation Secure Web Gateway), du CASB (Cloud Access Security Broker) et des principes Zero Trust, facilite et sécurise davantage l'expérience de vos utilisateurs lorsqu'ils sont dans le cloud.

Contexte : changer la donne en matière de sécurité

Un SASE efficace dépend du contexte ; et la plateforme Netskope intègre un générateur pour ce contexte enrichi. Dans Netskope, Cloud XD (abréviation de « *extreme definition* ») est le service contextuel qui transforme votre trafic Web, vos services cloud et l'activité de vos applications SaaS (Software as a Service) en informations intelligibles et exploitables. Cloud XD capture et décode les détails du trafic qui permettent d'identifier les utilisateurs, leurs appareils, les applications utilisées et les activités spécifiques de ces applications. Ces informations décodées sont partagées avec tous les services de sécurité, ce qui permet d'appliquer des stratégies de sécurité détaillées sur la base des indices fournis par Cloud XD.

Répondre aux questions de base

Les détails fournis par Cloud XD sont nombreux et variés, et dépendent eux-mêmes de l'activité spécifique en cours. Ces détails peuvent inclure les informations suivantes :

- L'utilisateur charge ou télécharge-t-il quelque chose ?
- Si oui, ce « quelque chose » inclut-il des données sensibles ?
- Combien d'octets l'utilisateur charge ou télécharge-t-il ?
- Quelle est l'application utilisée ?
- La personne utilise-t-elle une instance professionnelle ou personnelle d'une application ?

Ces exemples sont simples, mais vous serez peut-être surpris d'apprendre que, jusqu'à récemment, ces données de base et générales n'étaient pas réellement à la disposition des équipes de sécurité, et

qu'elles étaient loin de constituer une présentation agrégée et cohérente pouvant être appliquée à l'ensemble de l'infrastructure de sécurité.

La disponibilité de ces nouvelles informations permet de créer un récit sur l'activité d'un utilisateur pouvant ressembler au scénario suivant :

> Lauren utilise l'instance de Gmail de son entreprise et a obtenu l'accès à l'aide de ses identifiants de connexion professionnels : un nom d'utilisateur que vous connaissez, son mot de passe qui a été accepté et un code d'authentification à deux facteurs (2FA) qui a été accepté. Vous savez que Lauren a peut-être un compte Gmail personnel, et vous gardez donc la trace de l'instance avec laquelle elle travaille, car Gmail lui permet de changer facilement de compte dans la fenêtre de son navigateur.

ATTENTION

Le contexte, dans le sens d'une sécurité moderne et sophistiquée, exige que vos services de sécurité soient à l'affût des changements et des anomalies à *tout* moment. De nos jours, les pirates sont devenus très habiles dans la capture d'informations d'identification grâce au phishing via des applications SaaS et en lançant d'autres attaques axées sur le cloud, ce qui leur permet d'échapper plus facilement aux défenses web traditionnelles. Lorsque l'accès est accordé à un utilisateur, le travail de la sécurité ne fait que commencer !

Examiner le comportement

Le contexte précieux va au-delà des questions de base (auxquelles nous faisons référence dans la section précédente) en détectant et en évaluant les modèles de comportement après l'accès d'un utilisateur. Cloud XD applique des analyses sophistiquées à la recherche d'indices indiquant qu'un compte a été compromis, en révélant lorsqu'un (soi-disant) « utilisateur autorisé » s'engage dans une activité en dehors de son comportement habituel ou du rôle qui lui a été attribué. Cloud XD recherche des signes de comportement suspect pour répondre à des questions comme celles-ci :

- Cet utilisateur fait-il des choses qu'il ne fait pas normalement, comme déplacer des données ?
- L'utilisateur accède-t-il à des applications ou à des contenus différents de ceux qu'il utilise habituellement ?
- Quelle est la quantité de données que l'utilisateur charge ou télécharge, et cette activité ou cette quantité de données est-elle inhabituelle ?
- L'utilisateur interagit-il avec son appareil de manière atypique ?

RAPPEL

Les gens peuvent sembler imprévisibles, mais leurs routines et leurs modèles de travail sont reconnaissables. La NG-SWG développe un profil d'utilisateur au fil du temps et utilise ce profil pour détecter les actions hors norme, comme les mouvements de données inhabituels, les tentatives d'utilisation abusive des informations d'identification, et bien d'autres anomalies.

Creuser dans un contexte externe enrichi

Cette approche globale, axée sur le contexte, rend la sécurité du le cloud très intelligente. Vous en savez plus non seulement sur le contexte interne (l'utilisateur, l'appareil, le réseau et les applications qui sont tous « à l'intérieur » du réseau de l'entreprise), mais aussi sur ce qui se trouve à l'extérieur du réseau de l'entreprise. Netskope permet à une architecture SASE de mieux comprendre tout ce qui fait fonctionner le cloud, comme les interfaces de programmation d'applications (API), qui permettent aux applications de communiquer entre elles, et la notation d'objets JavaScript Object Notation (JSON), qui permet aux données d'avoir une structure flexible. Des services supplémentaires fournissent des informations contextuelles sur des sites web, des services cloud et des espaces de stockage de données spécifiques afin de brosser un tableau complet de l'environnement cloud dans lequel l'utilisateur travaille.

Pris dans son ensemble, ce contexte rend les services de sécurité plus efficaces. Étant donné que les services de sécurité en savent désormais plus, ils peuvent agir plus intelligemment. Les services peuvent être contrôlés par des stratégies qui définissent exactement ce qui est autorisé et ce qui ne l'est pas, jusqu'à des détails très spécifiques, et un contexte en constante évolution.

Découvrir comment les services sont plus grands que la somme de leurs parties

Par le passé, les appliances de sécurité fonctionnaient souvent séparément les unes des autres, en effectuant leurs tâches individuelles de manière séquentielle et isolée. En revanche, l'architecture rendue possible par Netskope et nécessaire pour un SASE efficace signifie que les services peuvent s'entraider en cas de besoin, ce qui rend l'ensemble de l'architecture plus intelligente. Les services de protection contre la perte de données (DLP) peuvent collaborer avec les services d'analyse du comportement des utilisateurs et des entités (UEBA) pour appliquer des niveaux supplémentaires de protection des données lorsqu'un utilisateur présente un comportement à risque. Par exemple, la reconnaissance optique de caractères (OCR), un service DLP avancé, peut être

utilisée pour détecter le contenu d'un document qu'un utilisateur charge et déterminer si le document peut être partagé en toute sécurité. Une collaboration gagnante !

Le profil de l'utilisateur oriente le processus, permettant, par exemple, à votre directeur financier de partager des informations avec le comptable de l'entreprise, tout en empêchant un responsable des activités de partager un sous-ensemble des mêmes informations avec un copain courtier en bourse.

Découvrir comment la sécurité fonctionne lorsque les utilisateurs constituent le périmètre

Avant le SASE, la sécurité des utilisateurs signifiait surtout une chose : pouvoir les identifier. Une fois l'utilisateur identifié, l'accès était accordé au-delà du périmètre à la « *forteresse* » (les données, applications et services que l'individu était autorisé à utiliser). En outre, la personne pouvait avoir des autorisations et des restrictions spécifiques dictant les éléments avec lesquels elle était autorisée à travailler, sans compréhension granulaire approfondie et certainement sans protection contre les comportements erratiques dans le cadre de ces engagements autorisés.

ATTENTION

Le SASE commence toujours par la gestion des identités et des accès, notamment via les processus habituels de nom d'utilisateur, de mot de passe et d'authentification multifactorielle que nous rencontrons tous quotidiennement dans notre univers digital. Mais dans une architecture SASE, tout ceci n'est que le début de la vérification de l'identité d'un utilisateur. Vos services de sécurité disposent désormais d'un profil d'utilisateur enrichi, détaillé et mis à jour en permanence, sur lequel ils peuvent s'appuyer. Toutes ces autres « éléments », y compris l'appareil qu'il utilise, l'heure de la journée, l'endroit où il se trouve, les applications qu'il utilise et la vitesse à laquelle il tape, fournissent beaucoup plus d'informations pour confirmer que l'utilisateur est bien celui qu'il prétend être. Même si les informations d'identification de base d'un utilisateur sont compromises, vos services de sécurité du SASE continuent de protéger votre entreprise et ses données. (Dans l'architecture de Netskope, ces renseignements sont également intégrés dans un score de risque pour l'utilisateur. Nous y reviendrons dans le chapitre 4).

Une idée largement approuvée dans les milieux de la sécurité est le *Zero Trust* : lorsque des utilisateurs ou des appareils essaient d'utiliser des applications et des données dans vos systèmes, on part du principe

qu'on ne peut pas leur faire confiance, du tout, jusqu'à ce qu'ils puissent prouver qu'ils sont bien ceux qu'ils prétendent être. Même dans ce cas, l'utilisateur n'est limité qu'à l'ensemble des ressources pour lesquelles il vient d'être approuvé. S'il essaie de faire autre chose, il devra à nouveau s'authentifier.

Les principes Zero Trust peuvent être appliqués de manière plus puissante aux architectures SASE et constituent un autre aspect essentiel de la bonne implémentation du SASE. L'idée est qu'avec tout le trafic réseau, que vous reconnaissiez ou non l'utilisateur, son appareil, etc., vous supposez toujours que l'utilisateur n'a pas que de bonnes intentions.

Le Zero Trust, et l'une de ses implémentations les plus connues, le Zero Trust Network Access ou ZTNA, ne sont pas nouveaux dans les cercles de sécurité des entreprises, mais le SASE élargit le champ d'application des principes Zero Trust. Avant le Zero Trust, une fois qu'un utilisateur était autorisé à entrer dans les services du datacenter, il pouvait être limité à un ensemble spécifique d'activités autorisées. Dans ces limites, il était essentiellement libre de faire ce qu'il voulait.

Le SASE rend les principes Zero Trust à la fois plus puissants et plus flexibles, voire permissifs, pour tous les utilisateurs globalement. (***N'oubliez pas :*** vos utilisateurs sont désormais le périmètre ! Et pour être honnête, ils constituent même plusieurs « périmètres »). L'architecture SASE applique le contexte dont disposent les utilisateurs sur l'ensemble du trafic pour prendre des décisions plus éclairées et plus granulaires sur ce que les utilisateurs peuvent et doivent être autorisés à faire. *À aucun moment* l'architecture SASE ne suppose que le trafic d'un utilisateur est légitime. Même si votre employé connu utilise une application SaaS que vous voulez qu'il utilise et qu'il travaille avec un ensemble de données qui correspond à sa fonction, vous ne pouvez pas simplement supposer que ce qu'il fait avec ces deux éléments est justifié.

RAPPEL

Si vous ne pouvez pas voir ce qui se passe dans votre trafic (les interactions et les transactions à l'intérieur des connexions qui ont été autorisées), votre sécurité est faible. En *rapprochant* la protection des utilisateurs, quel que soit l'endroit où ils accèdent aux données, et en distribuant des services à ces points d'accès en périphérie, votre sécurité peut voir à l'intérieur du flux de trafic sans obliger les utilisateurs à revenir vers votre datacenter. Les utilisateurs peuvent travailler de n'importe où, et la stratégie de sécurité peut être appliquée partout.

Reconnaître que la protection contre les menaces avancées est meilleure dans le cloud

La protection contre les menaces avancées (ATP) est une autre activité de sécurité existante dont la portée et l'efficacité sont considérablement accrues dans le cadre d'un SASE correctement implémenté. Jusqu'à récemment, l'ATP faisait uniquement référence aux approches adoptées pour protéger les utilisateurs contre les menaces entrantes, généralement sous la forme de fichiers malveillants.

Mais pour être efficace dans les flux de travail cloud, l'ATP doit également se concentrer sur les menaces basées dans le cloud, qui comprennent non seulement les fichiers malveillants, mais aussi les applications et les systèmes qui peuvent présenter des dangers. Dans le cloud, vous avez de nouveaux angles d'attaque à considérer, notamment :

- Les points de terminaison ou périphériques comme les ordinateurs portables, les tablettes, les téléphones et les capteurs et appareils de l'Internet des objets (IoT) qui transmettent des informations du monde extérieur à vos systèmes internes en utilisant une connexion cloud
- Le cloud, y compris les applications SaaS et les sites web : les bons, les mauvais et toutes les variantes intermédiaires, comme les services légitimes contrôlés par des acteurs malintentionnés
- Les utilisateurs, principalement l'évaluation et la vérification des personnes agissant au nom de votre société

L'efficacité de l'ATP dans le cloud nécessite une approche proactive. Elle doit empêcher les menaces d'agir lorsque cela est possible et détecter celles qui se manifestent le plus rapidement possible. (Netskope déploie en outre des services d'analyse par intelligence artificielle [IA]/Machine Learning [ML] pour amplifier sa capacité à reconnaître les problèmes).

La NG-SWG est à l'avant-garde pour aider à surmonter ce défi à grande échelle avec l'outil Netskope Cloud Threat Exchange, qui alimente vos services SASE avec un flux continu de renseignements actualisés sur les menaces, développés par *tous* les fournisseurs qui contribuent à votre plateforme SASE. Tout ceci vient compléter les renseignements obtenus par la NG-SWG, notamment l'expertise spécifique de la gestion des identités, de la protection des points de terminaison, des informations de sécurité, de la gestion des événements et d'autres services intégrés.

CONSEIL

La variété des vecteurs de menace possibles dans le cloud est considérable. Aucune organisation ne peut suivre le rythme à elle seule. Un SASE efficace est donc le résultat d'un travail d'équipe entre vos différents fournisseurs de services de sécurité.

Faire évoluer la SWG pour le cloud

Lorsque vous ne vous défendiez que contre les menaces web de base, votre infrastructure de sécurité comportait probablement une appliance permettant de bloquer l'accès des utilisateurs aux sites web non autorisés et de les empêcher de télécharger des malwares et d'autres éléments indésirables à partir du web. Principalement désignés par l'acronyme *SWG* et sous d'autres noms tels que *proxy web* ou *filtrage de contenu*, ces systèmes analysent activement les URL demandées par les utilisateurs, sont vigilants sur l'utilisation des applications de communication et surveillent le trafic entrant à la recherche de logiciels malveillants et de virus connus.

Bien entendu, vous avez toujours besoin de cette fonctionnalité, c'est pourquoi la NG-SWG (voir le chapitre 2) fournit ces services SWG de base. Mais grâce à sa gamme plus étendue de services d'inspection et à son accès à de vastes ressources contextuelles, la NG-SWG est bien plus à même de lutter contre les nouvelles menaces rendues possibles par le cloud. Par exemple, bien que la NG-SWG empêche toujours le téléchargement de logiciels malveillants, elle examine et surveille également le trafic lorsqu'une personne utilise Dropbox, Google Workspace, Microsoft Office 365 et tout autre service SaaS ou cloud. Cela permet de protéger l'environnement de travail, même s'il se trouve entièrement dans le cloud et que l'utilisateur n'a rien téléchargé sur un système d'entreprise local.

Si vous faites tout cela correctement, vos utilisateurs seront plus en sécurité et plus à même d'être efficaces dans leur travail. Vos employés sont donc protégés, et l'organisation en profite lorsque ses employés sont libres d'être productifs sans compromettre des actifs précieux ou se heurter à des problèmes de conformité et de gouvernance.

DANS CE CHAPITRE

- Changer les règles du jeu en matière de sécurité en définissant des stratégies générales
- Utiliser les superpouvoirs de la NG-SWG pour contrôler les données, quel que soit le point d'accès
- Relever le défi des applications et des services cloud non gérés
- Voir l'inspection single-pass en action
- Comprendre pourquoi le Zero Trust est essentiel pour une protection efficace des données

Chapitre 4
Protéger les données et les applications

Auparavant, la protection consistait à tout garder en sécurité à l'intérieur du périmètre de votre datacenter. Aujourd'hui, les données et les applications se trouvent hors de la forteresse de votre datacenter et dans le cloud. Il est temps d'abandonner définitivement certains concepts dépassés de la protection des données.

Ce chapitre examine comment la protection des données doit évoluer et comment la technologie Netskope SASE vous aide à garantir que les données sensibles de votre organisation ne sont pas utilisées à mauvais escient ou ne deviennent vulnérables.

Vaincre la complexité grâce à la puissance des stratégies

Par le passé, les équipes de sécurité étaient limitées non seulement par leurs compétences, mais aussi par leur portée. Leurs principales défenses étaient des piles d'appliances de sécurité disparates (pare-feux, passerelles web sécurisées (SWG), instances CASB, etc.). Par définition, les environnements de sécurité disjoints et les appliances

spécialisées sont limités. Pire encore, après avoir subi la microgestion nécessaire pour indiquer à chacune de ces boîtes spécialisées comment faire son travail, ces systèmes n'ont pas la visibilité, la portée ou la puissance nécessaires pour sécuriser correctement le cloud ou pour collaborer afin de prévenir les menaces et d'y répondre. Le seul choix possible est de bloquer l'accès (voir la figure 4-1), même si cette stratégie n'a pas de sens, car le contexte de l'utilisateur est disponible.

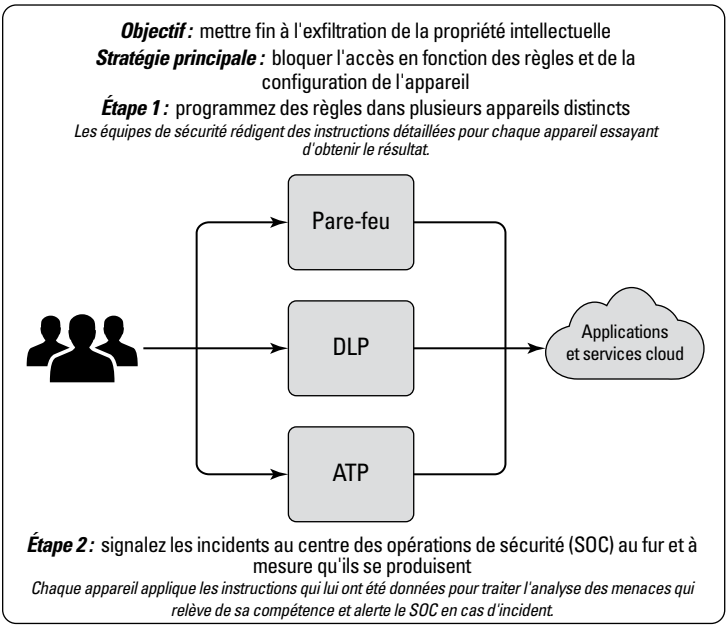

FIGURE 4-1 : Bloquer l'accès, quel que soit le contexte.

Netskope résout ce problème en remplaçant ce désordre incohérent (voir la figure 4-2). Elle permet à votre équipe de sécurité de définir de vastes stratégies au niveau macro, à savoir un ensemble cohérent d'instructions qui décrivent le résultat que vous souhaitez obtenir. La SWG de nouvelle génération (NG-SWG) permet de transformer ces instructions en actions, en coordonnant et en dirigeant les services de sécurité pour atteindre les résultats souhaités.

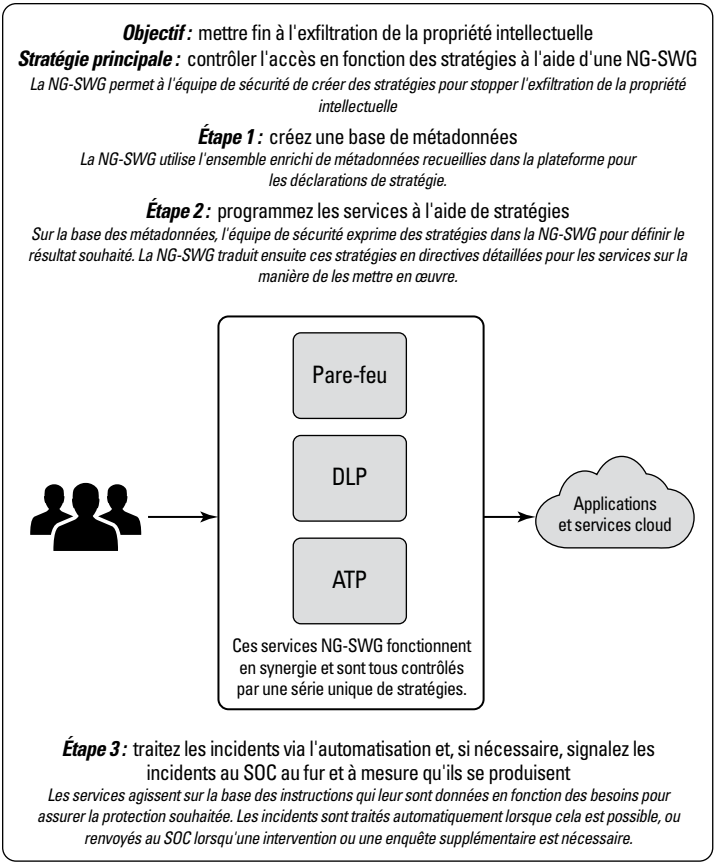

FIGURE 4-2 : Des stratégies plus étendues orientent les services de sécurité pour obtenir les résultats souhaités.

Contrairement à une approche rudimentaire de blocage ou d'autorisation, les contrôles de stratégies spécifiques qui prennent en compte le contexte et les nuances permettent de réduire le nombre d'appareils et de règles à gérer, et aux utilisateurs de s'engager davantage dans les applications et les services qui stimulent la productivité. Cette approche simplifie la vie de votre équipe de sécurité. Moins d'appareils à contrôler et moins de règles à rédiger, cela signifie moins de risques d'erreurs. Il est plus facile de maintenir et de modifier ce système en fonction de l'évolution des besoins. Même lorsque les systèmes sous-jacents sont mis à jour et améliorés, les stratégies restent les mêmes. Les services peuvent évoluer rapidement pour faire face aux nouvelles menaces, car les changements ne perturbent pas la structure de sécurité.

Protection des données

Avant l'avènement du Secure Access Service Edge (SASE), les systèmes de protection contre la perte de données (DLP) suivaient les données lorsqu'elles sortaient du réseau de l'entreprise afin d'éviter qu'elles ne soient utilisées ou partagées de manière non autorisée et de satisfaire aux exigences de conformité. Aujourd'hui, les données de l'entreprise résident de plus en plus en dehors de l'entreprise, parmi les services et les applications cloud ; elles se déplacent également à l'intérieur et entre les applications cloud, et parfois sans jamais passer par des points de terminaison.

Netskope surveille à la fois le trafic web et l'activité cloud pour sécuriser toutes ces données. La NG-SWG tire parti de toutes ces informations pour améliorer en permanence les services de sécurité. Des contrôles spécialisés lui permettent de savoir quel service cloud géré ou non géré est utilisé et si les utilisateurs se trouvent dans vos bureaux ou à distance. La NG-SWG reconnaît ce que les utilisateurs font au sein de chaque service et les activités entre les services (par exemple, si un employé télécharge des données sensibles au sein d'un service géré et essaie ensuite de charger ces données sur son compte Gmail personnel).

La NG-SWG met automatiquement en œuvre vos stratégies de sécurité pour protéger les données. Lorsque vous définissez une stratégie visant à interdire le partage d'informations confidentielles, la NG-SWG utilise son service DLP et ses classificateurs d'images pour déterminer si un utilisateur fait une capture d'écran d'une diapositive Microsoft PowerPoint confidentielle ou d'une image de tableau blanc contenant du texte confidentiel ; elle empêche alors cet utilisateur d'envoyer par courrier électronique ou de charger la capture d'écran vers des lecteurs partagés non gérés ou personnels ou de partager les données dans un formulaire web.

RAPPEL

L'intelligence artificielle (IA) et le Machine Learning (ML) renforcent la protection des données. Netskope NG-SWG utilise l'IA et le ML comme puissance de feu supplémentaire pour détecter les détails contextuels nuancés avec une plus grande précision. Ces technologies offrent des fonctionnalités spécialisées, notamment :

- **Détection de modèles et d'images :** utilisation d'algorithmes qui permettent de catégoriser les informations pour fournir une évaluation dynamique du risque des pages web ou détecter les documents malveillants et les images d'informations confidentielles

- **Détection des anomalies :** reconnaissance d'occurrences qui sont rares, inhabituelles ou autrement hors de propos dans les données ou les comportements

Les classificateurs spécialisés de l'IA ou du ML déterminent les types d'images qui sont déplacées pour reconnaître les contenus confidentiels comme les passeports, les images de tableaux blancs, les permis de conduire et les captures d'écran. D'autres analysent les types de documents pour détecter le code source, les curriculum vitae et d'autres sources de données protégées. Cette fonctionnalité constitue une amélioration puissante en termes de précision et d'efficacité de la sécurité des données, ce qui est important pour sécuriser le volume de données créé aujourd'hui.

Protection des applications

L'organisation d'aujourd'hui repose sur plusieurs catégories d'applications, notamment les applications gérées, les applications non gérées (ce que l'on appelle le *Shadow IT*), les services cloud publics et les applications personnalisées hébergées dans le cloud public.

Autrefois, les équipes de sécurité étaient en mesure de protéger les applications contre les menaces externes en maintenant simplement les pare-feux à jour. Plus tard, les pare-feux d'applications web ont ajouté davantage de protection. Mais cette protection était limitée aux applications web s'exécutant dans le datacenter.

Lorsque les applications cloud sont arrivées, les fournisseurs d'applications cloud ont été invités à fournir des interfaces de programmation d'applications (API) de gestion permettant aux départements informatiques de voir ce que les utilisateurs faisaient des applications et leur donnant un peu de contrôle. Ces applications, telles que Salesforce, ServiceNow et Workday, sont devenues des *applications gérées* ou *approuvées* (voir le chapitre 2).

Netskope a fourni l'un des premiers outils utilisés pour cette gestion : son CASB, qui utilise les API fournies par Google, Microsoft, Salesforce et d'autres fournisseurs pour donner accès à toutes les capacités de surveillance et de contrôle que ces développeurs d'applications ont incluses.

ATTENTION

Le problème pour les équipes de sécurité est que de nombreuses applications précieuses n'ont pas d'API de gestion publiées. Parfois, le personnel informatique pouvait évaluer la fiabilité, la sécurité et la sûreté de ces applications non gérées. Mais comme nous l'avons vu dans les chapitres précédents, les employés utilisent souvent l'application qu'ils souhaitent, ce qui entraîne une informatique souterraine non autorisée et non surveillée.

Avec la NG-SWG, cependant, et contrairement à la SWG traditionnelle, la fonctionnalité du CASB s'étend de façon spectaculaire. Les fonctionnalités d'inspection approfondie intégrées à Netskope Security Cloud surveillent le trafic HTTP/S (Hypertext Transfer Protocol/Secure) et API de *toutes les* applications web et cloud utilisées par vos employés. Cela comprend vos applications et vos services gérés et non gérés qui étaient auparavant invisibles pour le CASB. Le Shadow IT ou informatique souterraine entre dans la lumière !

Netskope peut découvrir des dizaines de milliers d'applications et de services cloud et leur attribuer une cote de risque. Cette évaluation du risque est basée sur l'indice de confiance dans le cloud de Netskope (Cloud Confidence Index), une mesure objective de l'état de préparation au risque d'un service cloud, dérivée des ressources de Netskope et d'une variété de services de renseignements sur les menaces du secteur. La NG-SWG utilise cette évaluation pour informer les utilisateurs et les équipes de sécurité et pour orienter l'application de vos stratégies de sécurité. Lorsqu'un utilisateur est connecté aux services cloud de votre organisation, comme Microsoft Office 365, son activité est surveillée afin qu'il ne puisse pas télécharger des données dans cette instance, puis les transférer vers une application cloud non gérée et risquée.

Voir Netskope en action

Le chapitre 2 décrit l'approche d'inspection single-pass de Netskope NG-SWG. Voici une description détaillée de la manière dont la NG-SWG applique cette approche pour sécuriser les données et les applications :

- **Étape 1 :** la NG-SWG identifie plusieurs instances de services et d'applications cloud pour différencier les instances personnelles, tierces et d'entreprise de la messagerie électronique et/ou des applications de productivité. Elle utilise le système d'évaluation Cloud Confidence Index de Netskope pour bloquer l'accès aux sites web malveillants, aux applications SaaS (Software as a Service) risquées et aux services cloud non sécurisés. Elle s'efforce activement d'empêcher la propagation des logiciels malveillants et d'autres menaces web sophistiquées.
- **Étape 2 :** à l'aide de métadonnées sur l'identité, l'emplacement, l'appareil et le réseau de l'utilisateur, la NG-SWG ajuste le niveau d'accès pour chaque session en fonction de ce contexte. Par exemple, si la NG-SWG détermine qu'un employé pleinement authentifié utilise une tablette personnelle sur un point d'accès Wi-Fi public, elle peut l'empêcher d'accéder à une application cloud critique et gérée.

- **Étape 3 :** la NG-SWG applique un contrôle sur les activités spécifiques des utilisateurs afin de réduire le risque de fuite et d'exposition des données. Les règles concernant le chargement et le téléchargement de documents, le partage de captures d'écran, le remplissage de formulaires web, ainsi que la création, la publication et la diffusion sur des services tels que les réseaux sociaux sont appliquées dans chaque application et instance.
- **Étape 4 :** la NG-SWG surveille en permanence toutes les activités autorisées par les étapes précédentes, à la recherche d'anomalies et de menaces. Elle reconnaît les données sensibles qui circulent et réagit à la volée en fonction de la sensibilité des données, du type d'action et d'autres paramètres pertinents. Les classificateurs d'images et les techniques de détection de modèles améliorés par le ML entrent en jeu. La NG-SWG peut bloquer certaines actions spécifiques, déclencher une alerte, interroger l'utilisateur sur ses objectifs, demander une authentification renforcée ou mettre en quarantaine des données pour une inspection plus approfondie par les équipes de sécurité. La NG-SWG offre un contexte très détaillé, de sorte que les faux positifs sont rares.

Elle implémente de manière étendue les principes directeurs d'un SASE correctement mis en œuvre afin que les données et les applications soient protégées, où qu'elles soient et quel que soit le lieu ou le mode d'accès.

L'importance des principes Zero Trust pour la protection des données

L'application des principes Zero Trust est l'une des évolutions les plus importantes de la sécurité des dix dernières années (voir le chapitre 3), et aucune discussion franche sur la protection des données ne serait possible sans elle. C'est l'idée qu'aucun utilisateur accédant aux données ne doit être intrinsèquement fiable, et que l'accès aux applications et aux données doit être limité au minimum. Les implémentations du Zero Trust telles que le Zero Trust Network Access (ZTNA) sont bien connues dans les milieux de la sécurité et de la gestion des réseaux. Mais que signifie Zero Trust pour la protection des données ?

RAPPEL

Comme d'autres infrastructures antérieures au cloud, la DLP a été fondée sur l'idée que tout ce qui est important se trouve à l'intérieur d'un datacenter, protégé par un périmètre réseau. Autrefois, la protection des données était chargée d'empêcher les fuites de données non autorisées et de bloquer l'accès des personnes non autorisées au périmètre pour accéder à ces données.

Cette approche n'est plus valable aujourd'hui à l'ère du cloud. Certaines données cruciales se trouvent dans le datacenter, derrière le périmètre traditionnel, mais au moins autant (et de plus en plus) de données se trouvent dans les applications SaaS et dans les applications hébergées dans le cloud public. Les organisations doivent repenser la protection des données en fonction de la façon dont les utilisateurs travaillent de nos jours, afin de protéger une surface d'attaque beaucoup plus large et beaucoup plus dynamique. Il leur faut un moyen d'accorder aux utilisateurs l'accès aux données dont ils ont besoin, au moment où ils en ont besoin, et rien de plus.

En 2021, Netskope a décrit pour la première fois l'expression *Protection des données Zero Trust* en tant qu'approche de la sécurité qui fournit un contrôle continu et en temps réel de l'accès et des stratégies en fonction du risque et du contexte. Le contexte vous aide à comprendre les interactions entre les utilisateurs et les applications et vous informe sur la manière d'autoriser et d'empêcher l'accès aux données en fonction d'une compréhension approfondie de l'identité de l'utilisateur, de ce qu'il essaie de faire et de la raison pour laquelle il le fait. C'est ce qui permet aux équipes de sécurité de définir et d'appliquer des contrôles conditionnels en fonction de la sensibilité des données, du risque lié à l'application, du risque lié au comportement de l'utilisateur et d'autres facteurs ; et de faire tout cela en temps réel. Il en résulte une sécurité plus efficace, grâce à une gestion continue des risques.

Une approche de gestion continue des risques est le seul moyen efficace de gérer les risques de façon dynamique sur un ensemble d'applications tierces lorsque vous disposez d'une main-d'œuvre principalement distante qui a besoin d'un accès permanent aux applications cloud et aux données pour rester productive (voir le chapitre 2).

RAPPEL

La protection des données *Zero Trust* n'est pas seulement une nouvelle façon d'envisager la DLP ou de créer un concept marketing de plus pour profiter de la popularité du Zero Trust. La protection des données Zero Trust est la véritable incarnation d'une implémentation optimale du SASE, qui consiste à transformer la sécurité et les réseaux pour répondre aux besoins actuels d'accès omniprésent au cloud et à garantir que les données sont protégées partout. Une approche unifiée et complète du SASE et de la protection des données Zero Trust permet de distinguer les véritables fournisseurs de technologie SASE des amateurs.

DANS CE CHAPITRE

- Bien comprendre la politique de sécurité cloud de votre entreprise
- Améliorer l'évaluation des risques en observant l'activité en dehors de votre datacenter
- Contrôler qui déplace quelles données et à quel endroit
- Habiliter et sécuriser entièrement votre main-d'œuvre à distance et à grande échelle
- Remanier votre datacenter pour travailler en toute sécurité avec le cloud

Chapitre 5
Dix étapes (ou moins) pour accéder au SASE

Ce chapitre présente une approche étape par étape de l'implémentation du Secure Access Service Edge (SASE), du point de départ jusqu'à l'optimisation et en passant par toutes les étapes intermédiaires.

Il donne un aperçu de la manière dont vous pouvez réussir le déploiement du SASE en sept étapes. À chaque étape, vous ferez de grands progrès pour améliorer considérablement la sécurité de votre organisation, gérer les risques et offrir à vos employés et à vos clients l'expérience dont ils ont besoin.

Étape 1 : déterminez vos objectifs

Lors de la mise en œuvre d'un nouveau projet, la nécessité de produire des résultats quantifiables aujourd'hui (ou du moins très rapidement !) est un défi majeur pour un directeur informatique (CIO), un directeur de la sécurité informatique (CISO) ou toute personne ayant des responsabilités importantes en matière de gestion réseau et de sécurité

d'entreprise. Contrairement aux projets informatiques typiques, pour lesquels de longs cycles de développement peuvent être tolérés, la sécurité doit démontrer sa valeur immédiatement et offrir des gains rapides. La vulnérabilité est effrayante.

Le SASE s'attaque à cette vulnérabilité en utilisant une architecture qui reflète la manière dont la sécurité doit être assurée *aujourd'hui* et la convergence croissante (et favorable) de la sécurité et des réseaux. Mais le véritable SASE est un processus d'évolution à long terme. Votre entreprise adoptera une architecture SASE au fur et à mesure. La clé de votre réussite réside dans une succession de victoires tangibles (des bonds en avant délibérés) qui étendent et renforcent de manière répétée la sécurité de votre organisation de façon réellement pertinente.

Mais pour ce faire, vous devez savoir par où commencer et où vous allez.

En abordant le SASE comme une série d'investissements et d'implémentations éclairés, chacun changeant la donne à lui seul, vous pouvez obtenir des résultats continus et spectaculaires en éloignant votre entreprise de sa vision désuète du monde centrée sur le datacenter pour en faire une entreprise capable de tirer parti pleinement et en toute sécurité des nombreux avantages du cloud.

Étape 2 : obtenez davantage d'informations et de visibilité

La première étape pour résoudre un problème est d'admettre qu'il y en a un. Ce livre explique comment la sécurité des entreprises n'a pas progressé au rythme des besoins actuels en matière de sécurité et d'accès, mais est plutôt restée ancrée dans le datacenter traditionnel.

Plus de la moitié des utilisateurs et du trafic des applications d'entreprise utilisent des réseaux que l'entreprise ne contrôle pas, et ce, avant que la pandémie de COVID-19 ne fasse du télétravail la nouvelle norme (voir chapitre 1).

Vous et votre organisation devez prendre conscience de la gravité et de l'ampleur de ce qui a échappé à votre contrôle, et du fait que ce qui échappe à votre contrôle est la façon dont votre entreprise fonctionne aujourd'hui. L'implémentation de la NG-SWG de manière élémentaire, même pour un seul service, vous permettra d'y voir plus clair, d'avoir une visibilité sur ce qui se passe et ce qui n'est pas protégé.

CONSEIL

Au minimum, vous avez besoin d'une entière visibilité sur l'activité des utilisateurs dans le cloud si vous voulez avoir confiance dans toute solution que vous implémentez. Il faut également que les décideurs de votre organisation participent à cette initiative. Vous obtiendrez l'adhésion de ces décideurs lorsqu'ils comprendront que le SASE protégera des éléments stratégiques auxquels ils tiennent, mais dont ils ne se rendent pas compte qu'ils sont dangereusement exposés. Des millions, voire des milliards de dollars de valeur sont dérivés du travail effectué « en externe ».

Étape 3 : placez des points d'inspection centraux entre les utilisateurs et les applications

Avec la NG-SWG fermement mise en place et votre visibilité sur l'ensemble de votre trafic considérablement accrue, une chose est sûre : vous n'apprécierez pas forcément ce que vous verrez.

Vos collaborateurs utilisent-ils Microsoft Office 365 ? Salesforce ? Workday ? Box ? La réponse est presque certainement oui. Mais quelle est la taille et la maturité de cet environnement cloud au-delà de votre périmètre de sécurité et de ce que vous pouvez facilement voir ? Quel est le volume de données de votre entreprise qui circule sans être contrôlé ?

Pour la première fois, votre organisation sera consciente de l'ampleur du risque auquel elle était exposée. Vous verrez les flux de données, dont certains peuvent être particulièrement sensibles, entre les sites, services et applications non sécurisés.

Vous disposez maintenant d'une image fidèle, et probablement inquiétante, de la situation de votre organisation en ce qui concerne sa dépendance vis-à-vis de l'environnement cloud. Tant d'applications et de services, mais si peu de contrôles de sécurité efficaces. Jusqu'à aujourd'hui.

La NG-SWG établit un point d'inspection central single-pass, en forme d'entonnoir, pour tout votre trafic dans le cloud et dans le datacenter (voir le chapitre 2). Ce point d'inspection central est plus efficace que votre ancien périmètre. Sans aucun doute.

RAPPEL

Que ce soit le résultat du Shadow IT qui a été sciemment ignoré ou d'un processus plus délibéré de digitalisation des activités, vos systèmes de sécurité anciens et dépassés n'ont pas fait attention aux détails. En remplaçant les anciennes SWG et appliances similaires, vous disposerez

enfin d'une visibilité complète sur les personnes qui utilisent des applications et des services non professionnels et sur les données d'entreprise qui sont envoyées en externe et qui échappent à votre contrôle. Comme le montre le tableau 5-1, la NG-SWG et ses nouveaux points d'inspection dans le cloud vous permettent de voir ce qui se passe à l'intérieur de tout ce trafic : web, SaaS géré, applications en Shadow IT, services cloud publics et applications personnalisées dans le cloud public.

TABLEAU 5-1 Utilisation des points d'inspection pour surveiller le trafic

Oubliez les anciennes solutions	Adoptez Netskope	Netskope s'intègre à...
Ancienne SWG : accepte ou refuse uniquement le trafic web.	Inspection approfondie de tout le trafic : web, SaaS géré, applications en Shadow IT, services cloud publics et applications personnalisées dans le cloud public.	Solution d'authentification unique (SSO)
Appliance SSL (Secure Sockets Layer).	Le déchiffrement SSL/Transport Layer Security (TLS) est effectué dans le cloud à l'échelle du cloud sans aucune appliance requise.	
L'ancienne plateforme CASB surveille uniquement les applications gérées qui fournissent des interfaces de programmation d'applications (API).	Surveille les applications gérées ainsi que les applications non gérées qui n'offrent pas d'API ; voit également quelles données sont utilisées par les applications, les services et les sites web.	

Étape 4 : appliquez les principes Zero Trust au web, au cloud et à l'accès aux activités

C'est là que vous commencerez vraiment à mettre en œuvre votre technologie en jetant les bases de votre SASE. Heureusement, les capacités nécessaires pour remettre les choses en ordre sont intégrées à la plateforme Netskope. Vous disposez de tout ce dont vous avez besoin pour rétablir le contrôle de vos données d'entreprise, non seulement sur votre propre réseau mais aussi, à terme, partout dans le cloud.

À l'étape 3, comme le montre le tableau 5-2, vous utiliserez des contrôles de sécurité étendus pour appliquer le contexte, en allant au-delà des fonctions d'acceptation ou de refus utilisées par vos anciennes appliances. La NG-SWG procède également à des inspections approfondies de votre trafic web *et* de votre trafic cloud. Et maintenant que vous avez établi un nouveau point d'inspection, sa fonctionnalité est étendue pour exercer un contrôle fin sur le mouvement des données et leur accès afin de gérer le risque selon des stratégies qui ont du sens pour votre entreprise.

TABLEAU 5-2 Définition des politiques de gestion des risques

Oubliez les anciennes solutions	Adoptez Netskope	Netskope s'intègre à...
Ancienne fonctionnalité de protection contre la perte de données (DLP) : protège uniquement les données du datacenter.	La fonction DLP intelligente protège toutes les données déplacées, où qu'elles se trouvent.	Les systèmes de gestion des informations et des événements liés à la sécurité et aux systèmes de protection des points de terminaison.
Analyse du comportement des utilisateurs et des entités (UEBA)	Détection étendue des anomalies de comportement et évaluation du risque pour l'utilisateur.	
Diverses solutions de sandboxing.	Protection avancée contre les menaces (ATP), y compris le sandboxing et la détection des anomalies basée sur le Machine Learning.	

Étape 5 : étendez les principes Zero Trust à la protection des données et à l'accès privé

Maintenant que votre organisation connaît mieux son trafic, qu'elle a une visibilité et est à même d'appliquer des stratégies pour sécuriser ses données, vous pouvez tirer parti de tous les avantages du télétravail. Vous allez permettre au personnel de travailler de n'importe où et pourrez fournir une expérience formidable, fluide, productive et hautement protectrice de vos données, de vos applications et de vos employés.

Le changement le plus notable est l'abandon de l'ancien réseau privé virtuel (VPN) : ce routage long et inefficace de type *hairpinning* qui obligeait tout le trafic de vos utilisateurs distants à revenir au datacenter

avant d'atteindre l'Internet. Grâce à Netskope NewEdge, vous pouvez acheminer efficacement ce trafic vers sa destination tout en appliquant vos stratégies de sécurité pour protéger les données.

RAPPEL

Zero Trust signifie qu'il faut appliquer l'hypothèse selon laquelle tout utilisateur peut être malveillant à tout moment et veiller à ce que les données soient toujours protégées, où qu'elles aillent. Les connaissances contextuelles approfondies de la plateforme Netskope sur l'utilisateur, l'appareil, le réseau, le comportement et des centaines d'autres détails sont utilisées pour limiter l'activité à ce qui a été autorisé par la stratégie et pour s'assurer que l'utilisateur est bien celui qu'il prétend être.

Après sa mise en place, votre sécurité et votre réseau seront transformés pour répondre aux besoins des travailleurs dans le cloud et de la sécurité des données (voir le tableau 5-3).

TABLEAU 5-3 Sécurité et réseaux qui répondent aux besoins des collaborateurs distants

Oubliez les anciennes solutions	Adoptez Netskope	Netskope s'intègre à...
Ancien VPN	Sécurité dans le cloud pour acheminer et protéger le trafic en fonction des stratégies	Fournisseurs SD-WAN (Software-Defined Wide-Area Networking)
	Accès « Zero Trust » au réseau (ZTNA)	Systèmes de gestion des identités pour gérer et vérifier les identités des utilisateurs et des groupes
	Protection des données Zero Trust	

Étape 6 : redéfinissez les contrôles internes du datacenter pour une gestion des risques en boucle fermée

RAPPEL

Le datacenter n'est qu'une destination parmi d'autres pour les personnes et les données. Il n'est plus le centre d'intérêt. Lorsque vous êtes bien avancé dans votre architecture SASE, il est temps de reconsidérer l'objectif du datacenter.

Vous laisserez peut-être dans le datacenter quelques applications trop lourdes à déplacer ou trop précieuses pour être perdues de vue. Pour

accéder à ces applications, vous pouvez utiliser Netskope Private Access, qui élimine le VPN tout en offrant un accès sécurisé dans le monde entier.

Qu'en est-il des autres éléments qui ont été remplacés par les services de la plateforme Netskope dans une architecture SASE ? Profitez de cette occasion pour réduire considérablement la complexité et les coûts de maintenance de votre réseau, et laissez les anciens systèmes du passé se déprécier et disparaître, tandis que vous et votre entreprise regardez vers l'avenir.

Le tableau 5-4 indique quels anciens systèmes ou technologies désuètes peuvent être remplacés par la plateforme Netskope.

TABLEAU 5-4 Fournir un accès sécurisé au datacenter

Oubliez les anciennes solutions	Adoptez Netskope	Netskope s'intègre à...
Pare-feux, système de prévention des intrusions (IPS), DNS (Domain Name System)	Fournit des protections de pare-feu comme l'un des nombreux services	Contrôles des datacenters existants en entrée

Une véritable architecture SASE permet de réaliser des économies permanentes sur les coûts opérationnels. Le tableau 5-5 donne un aperçu de ce à quoi peut ressembler une architecture SASE réussie. Vos responsables financiers seront parmi les nombreuses parties prenantes à vous remercier !

TABLEAU 5-5 Économies permanentes sur les dépenses opérationnelles

Domaine	Ce qui se passe	Estimation des économies
Accès multicloud	Activation de la stratégie multicloud Amélioration de l'expérience utilisateur Rationalisation de l'approvisionnement et de l'adoption Activation des applications dirigées par des divisions métier	30 % sur la connexion et l'infrastructure 20 % sur les coûts futurs du cloud

(suite)

TABLEAU 5-5 *(suite)*

Domaine	Ce qui se passe	Estimation des économies
Remplacement du VPN	Suppression des appliances VPN Trafic direct sur le réseau pour les applications gourmandes en bande passante Réduction des changements de stratégie en matière de réseau local virtuel (VLAN) et de pare-feu	80 % sur le matériel 50 % sur les changements de sécurité et l'administration
Partenaires commerciaux	Gestion de l'accès des tiers Accès direct aux applications publiées Application des contrôles granulaires pour l'activité Suppression des possibilités de mouvement latéral	80 % sur le matériel 20 % sur le temps d'assistance
Fusions et acquisitions (F&A)	L'intégration devient plus efficace Consolide les coûts actuels et futurs du réseau et de la sécurité Synchronise la stratégie	40 % sur le matériel L'intégration est cinq fois plus efficace

Étape 7 : contrôlez, évaluez et optimisez

Le chemin vers le SASE prendra du temps, mais ce modèle offre des avantages considérables et transformateurs à vos équipes de sécurité et à votre organisation à chaque étape. La sécurité s'améliore certainement tout au long de votre parcours, mais l'impact va bien au-delà. Vous commencerez rapidement à réaliser des économies, car les appliances de sécurité existantes n'auront plus besoin d'être entretenues, mises à niveau et remplacées. Mieux encore, comme vous êtes entièrement optimisé pour le cloud, vous n'avez pas besoin d'acheter des appliances de sécurité coûteuses en capital et dotées d'une capacité excessive et inutilisée.

Mais la façon dont le SASE fonctionne dans votre entreprise sera différente de celle d'une autre entreprise, même si les principes qui sous-tendent le SASE sont les mêmes. Pour maintenir votre SASE opérationnel,

vous devez surveiller son fonctionnement, évaluer les améliorations nécessaires et prendre des mesures pour optimiser votre implémentation.

En prenant le temps de vous améliorer en permanence, vous protégerez vos acquis. Il est difficile de surestimer les avantages que la NG-SWG, en tant que plateforme, apporte à la sécurité des entreprises. Là où votre équipe de sécurité était débordée, essayant de comprendre et de corréler ce qu'une dizaine ou plus d'applications de sécurité complexes et indépendantes essayaient de lui dire dans le feu de l'action, elle disposera désormais d'une plateforme unifiée et automatisée fonctionnant en temps réel. Tous les services de sécurité délivreront un message commun et cohérent, ce qui réduira les erreurs et permettra d'agir de manière décisive et immédiate. Chaque membre de votre équipe sera en mesure d'en faire plus pour renforcer la sécurité et permettre à votre entreprise de fonctionner correctement.

Mais surtout, un SASE correctement architecturé doté d'une NG-SWG transformera les opérations commerciales et les relations entre les employés et la technologie, ainsi qu'entre vos équipes chargées de la gestion du réseau et de la sécurité. Les solutions en Shadow IT peuvent être utilisées au grand jour, permettant une véritable transformation digitale où les applications et les outils les plus performants peuvent être adoptés rapidement et en toute sécurité pour booster l'efficacité et stimuler les opportunités. L'expérience utilisateur sera préservée, et vos utilisateurs seront heureux et productifs. Tout cela n'est possible que lorsque le service chargé de la sécurité peut soutenir en toute confiance l'innovation numérique et l'adoption généralisée des services cloud et s'aligner sur les réseaux et toutes les parties de l'entreprise pour respecter les priorités de la transformation digitale. C'est ce que vous obtenez avec une véritable architecture SASE.

La plateforme de sécurité intelligente de l'ère SASE

Netskope, leader du SASE, connecte rapidement et en toute sécurité les utilisateurs directement à Internet, à toute application et à leur infrastructure à partir de n'importe quel appareil, dans ou hors du réseau. Avec CASB, SWG et accès Zero Trust intégrés nativement dans une seule plateforme, Netskope est performant partout, centré sur les données et orienté vers le cloud, tout en assurant une bonne gouvernance numérique et un faible TCO.

Pour plus d'informations,
visitez www.netskope.com/fr

netskope

Créez une architecture SASE qui protège les données et génère une valeur commerciale durable

Dans un monde digital qui a quitté les limites restrictives du datacenter pour les possibilités très ouvertes du cloud, une architecture SASE (Secure Access Service Edge) est la seule architecture qui ait du sens. Donnez à vos utilisateurs les moyens d'agir, protégez vos données et développez votre activité grâce à une architecture SASE bien conçue, qui combine les principes des services CASB (Cloud Access Security Broker), NG-SWG (Next-Generation Secure Web Gateway) et Zero Trust pour garantir la réussite de votre entreprise.

À l'intérieur…

- En savoir plus sur l'évolution des données, des applications, des réseaux et de la sécurité
- Comprendre les rôles du CASB, de la NG-SWG et du Zero Trust dans l'architecture SASE
- Sécuriser vos collaborateurs distants et mobiles à grande échelle et améliorer l'expérience globale de vos utilisateurs
- Élaborer un plan solide pour l'avenir de votre sécurité et de votre réseau

netskope

Les dirigeants de Netskope, **Jason Clark** (CSO), **Lamont Orange** (CISO) et **Steve Riley** (Field CTO), sont des références largement reconnues dans les domaines du cloud, de la sécurité et des réseaux, avec des décennies d'expérience au sein d'organisations internationales, notamment Ernst & Young, Gartner, Optiv, Riverbed et Websense.

Rendez-vous sur Dummies.com®
pour voir des vidéos, des exemples pas à pas, des articles pratiques, ou pour faire des achats !

ISBN: 978-1-119-85520-0

pour les nuls®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.