UN APPRENTISSAGE FACILE

Une édition spéciale de Palo Alto Networks

Accès réseau Zero Trust

pour les nuls®

Découvrez pourquoi le VPN n'est plus d'actualité

Accordez un véritable accès avec un minimum de privilèges grâce au ZTNA 2.0

Comprenez les limites de l'ancien ZTNA

Proposé par

paloalto® NETWORKS

Lawrence Miller

À propos de Palo Alto Networks

Palo Alto Networks est le leader mondial de la cybersécurité. Nous innovons pour déjouer les cybermenaces et pour que les organisations puissent adopter les nouvelles technologies en toute confiance. Nous fournissons une cybersécurité de nouvelle génération à des milliers de clients dans le monde entier, dans tous les secteurs. Nos plateformes et services de cybersécurité, les meilleurs de leur catégorie, s'appuient sur une surveillance hors pair des menaces et sont renforcés par une automatisation de pointe. Qu'il s'agisse de déployer nos produits pour créer une entreprise appliquant les principes du Zero Trust, de répondre à un incident de sécurité ou de s'associer pour obtenir de meilleurs résultats en matière de sécurité grâce à un puissant écosystème de partenaires, nous nous engageons à faire en sorte que chaque jour soit plus sûr que le précédent. C'est pourquoi nous sommes le partenaire privilégié en matière de cybersécurité.

Chez Palo Alto Networks, nous nous engageons à réunir les meilleures personnes au service de notre mission. Nous sommes donc également fiers d'être le lieu de travail préféré dans le secteur de la cybersécurité, reconnu parmi les lieux de travail les plus appréciés de Newsweek (2021), les meilleures entreprises pour la diversité de Comparably (2021) et les meilleurs endroits pour l'égalité LGBTQ de HRC (2022). Pour de plus amples informations, consultez www.paloaltonetworks.com.

Accès réseau Zero Trust

pour les nuls®

Accès réseau Zero Trust

Une édition spéciale de Palo Alto Networks

par Lawrence Miller

pour les nuls®

Accès réseau Zero Trust pour les Nuls®, une édition spéciale de Palo Alto Networks

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

ISBN 978-1-394-18372-2 (pbk) ; ISBN 978-1-394-18373-9 (ebk)

Pour obtenir des renseignements généraux sur nos autres produits et services, ou sur la publication d'un livre sur mesure *pour les Nuls* destiné à votre entreprise ou organisation, veuillez contacter notre service de développement commercial aux États-Unis, par téléphone au 877-409-4177, par e-mail à info@dummies.biz, ou consulter notre site www.wiley.com/go/custompub. Pour obtenir des informations sur la licence de la marque *pour les Nuls* pour des produits ou services, veuillez contacter BrandedRights&Licenses@Wiley.com.

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

Responsable de compte client : Cynthia Tweed

Éditeur de production : Magesh Elangovan

Assistance spéciale : Don Meyer, Shannon Bonfiglio

Table des matières

Introduction

La façon dont nous travaillons et le lieu où nous travaillons ont changé de façon spectaculaire en un laps de temps relativement court. Les initiatives de transformation numérique qui étaient déjà en cours avant la pandémie de COVID-19, comme le télétravail et le cloud computing, ont été soudainement et nécessairement accélérées pour faire face aux nouvelles réalités du monde moderne. Nous vivons désormais dans un monde où le travail n'est plus un endroit où l'on va. Au contraire, c'est une activité que nous pratiquons partout.

En raison de cette nouvelle norme, notre surface d'attaque s'est accrue de façon exponentielle, de nombreuses architectures prenant désormais en charge les connexions directes aux applications sur Internet au lieu d'acheminer le trafic vers les data centers via des réseaux privés. La connectivité VPN d'accès à distance traditionnelle ne fonctionne plus dans un univers où les utilisateurs et les applications se trouvent désormais en dehors des réseaux d'entreprise et des data centers. Les anciens VPN d'accès à distance offrent trop d'accès avec peu ou pas de détection des menaces ou des vulnérabilités, ce qui rend les ressources privilégiées vulnérables à la compromission des comptes d'utilisateurs. Face à l'augmentation spectaculaire du volume, de l'ampleur et de la sophistication des cyberattaques, les entreprises qui utilisent le cloud s'efforcent de combler leurs « lacunes » en matière de sécurité et ont commencé à se tourner vers des solutions d'accès réseau Zero Trust (ZTNA) pour réduire leur surface d'attaque et protéger leurs activités contre les ransomwares et autres exploits.

Cependant, les solutions ZTNA existantes (ou 1.0) ne sont pas en mesure de répondre aux besoins de sécurité des entreprises d'aujourd'hui. Elles fournissent un accès trop large avec une protection insuffisante, confèrent une sécurité inégale et incomplète pour les applications web et non web, et offrent des performances et une expérience utilisateur médiocres. Par conséquent, elles ne sont pas en mesure de faire face à l'assaut de nouvelles attaques toujours plus sophistiquées sur nos surfaces de plus en plus étendues.

Les solutions ZTNA 2.0 sont apparues comme la meilleure voie à suivre, inaugurant une nouvelle ère d'accès sécurisé dans un monde où le travail est une activité et non un lieu.

À propos de ce livre

L'*Accès réseau Zero Trust pour Les Nuls*, une édition spéciale de Palo Alto Networks, comporte cinq chapitres qui explorent les thèmes suivants :

- L'évolution du paysage de la sécurité, les bases du ZTNA et la nécessité d'aller au-delà du ZTNA 1.0 (chapitre 1)
- Comment le ZTNA 2.0 répond aux limites des solutions ZTNA actuelles (chapitre 2)
- Les facteurs essentiels de succès à rechercher dans une solution ZTNA 2.0 (chapitre 3)
- Les nprincipaux cas d'utilisation du ZTNA 2.0 et les témoignages de clients (chapitre 4)
- Les questions essentielles à poser à votre fournisseur ZTNA (chapitre 5)

Chaque chapitre est rédigé de façon indépendante du reste de l'ouvrage. Si un sujet vous intéresse, vous pouvez donc passer directement au chapitre qui s'y rapporte. Vous pouvez lire cet ouvrage dans le sens qui vous convient, mais nous vous déconseillons de le lire à l'envers ou de droite à gauche.

Il comprend également un glossaire pratique au cas où certains termes ou acronymes utilisés dans ce livre vous échapperaient.

Quelques suppositions

On dit que la plupart des hypothèses ont perdu leur utilité, mais je vais tout de même en faire quelques-unes.

Je suppose que vous êtes un décideur ou un professionnel en matière de nouvelle technologie et que vous êtes à la recherche d'une solution innovante pour fournir un accès sécurisé à vos effectifs hybrides. Que vous soyez directeur de la sécurité informatique (RSSI), directeur informatique ou ingénieur réseau ou sécurité, ce livre illustre comment le ZTNA 2.0 peut vous aider à relever les défis d'une surface d'attaque considérablement étendue et d'un paysage de menaces de plus en plus hostile.

Icônes utilisées dans ce livre

Tout au long de ce livre, j'utilise des icônes particulières pour attirer l'attention du lecteur sur certaines informations importantes. Attendez-vous donc à voir celles-ci :

RAPPEL

Cette icône signale des informations importantes à inscrire obligatoirement dans votre mémoire non volatile, votre matière grise ou votre crâne.

JARGON TECHNIQUE

Cette icône explique le jargon qui se cache derrière le jargon ; il s'agit de l'étoffe dont les héros (les nerds) sont faits !

CONSEIL

Les conseils sont appréciés, jamais attendus. Nous espérons que vous apprécierez ces informations utiles.

ATTENTION

Ces alertes soulignent les choses contre lesquelles vos parents vous ont mis en garde. En fait, probablement pas, mais elles offrent des conseils pratiques.

Au-delà de ce livre

Ce sujet est tellement vaste qu'il est impossible de tout aborder dans ce livre. Donc, si en arrivant à la fin du livre, vous vous demandez : « Où puis-je en savoir plus ? », il vous suffit de vous rendre sur `www.paloaltonetworks.com/sase/ztna`.

DANS CE CHAPITRE

- Analyser l'évolution du paysage de la sécurité
- Reconnaître la nature changeante du travail
- Comprendre les fondamentaux du Zero Trust
- Examiner les limites du ZTNA 1.0

Chapitre 1
Reconnaître les implications de la nouvelle norme en matière de sécurité

Ce chapitre explore les défis modernes en matière de sécurité, notamment l'augmentation des menaces, la complexité de l'écosystème de la sécurité et la pénurie de talents dans le domaine de la cybersécurité. Il explique également les bases de l'accès réseau Zero Trust (ZTNA) et pourquoi les organisations doivent aujourd'hui adapter leurs stratégies d'accès à distance pour s'aligner sur les nouveaux modèles de travail et évoluer au-delà des solutions de contrôle d'accès traditionnelles.

Regard sur un paysage en mutation

Le paysage moderne de la sécurité continue d'évoluer, car les menaces sont de plus en plus sophistiquées et fréquentes. En réponse à ces menaces, les organisations ont déployé un éventail toujours

plus large et vertigineux de solutions et d'outils de sécurité ponctuelle. Or, la gestion et l'exploitation de ces outils cloisonnés exigent souvent des compétences et des ressources spécialisées dont la plupart des équipes de sécurité des entreprises ne disposent tout simplement pas.

Des menaces toujours plus sophistiquées et fréquentes

Les fuites de données et les attaques par ransomware sont aujourd'hui si fréquentes qu'elles méritent pratiquement leur propre colonne dans les journaux, aux côtés de la météo, du sport et du trafic routier. Cependant, le fait que ces événements de sécurité soient courants ne les rend pas moins dangereux pour autant. Les organisations qui se montrent complaisantes en matière de sécurité risquent de subir des dommages considérables en cas d'attaque.

ATTENTION

Selon le Ponemon Institute, entre 2020 et 2021, le coût moyen d'une fuite de données a augmenté de 10 % pour atteindre 4,24 millions de dollars. Il s'agit de la plus forte augmentation annuelle des coûts au cours des sept dernières années.

Malheureusement, les équipes de sécurité des entreprises doivent mener une bataille difficile face aux tactiques, techniques et procédures (TTP) de plus en plus sophistiquées des cybercriminels.

RAPPEL

La capacité d'une organisation à rester à la pointe du paysage des menaces modernes nécessite des outils efficaces et une équipe d'analystes de sécurité compétente. Malheureusement, la plupart des organisations ont rarement instauré un bon équilibre entre la technologie et les experts qualifiés.

Trop d'outils et trop de complexité

Depuis de nombreuses années, les équipes de sécurité des entreprises déploient des solutions de sécurité ponctuelles pour répondre à des problèmes spécifiques et à des cas d'utilisation limités. Cela a souvent été décrit à tort comme une « défense en profondeur ». Hélas, l'écosystème de la sécurité est parsemé d'une multitude d'outils qui créent un environnement opérationnel complexe, coûteux et inefficace. Selon une étude IBM de 2020, l'entreprise moyenne utilise 45 outils de sécurité, et 30 % des organisations en utilisent plus de 50. Selon le *rapport Panaseer 2022 Security Leaders Peer Report* cité par *InfoSecurity Magazine*, « le passage au cloud et au télétravail a entraîné, au cours de ces deux dernières années, une

augmentation de 19 % du nombre d'outils de sécurité que les organisations doivent gérer, soit 76 au lieu de 64 ».

Ces outils de sécurité génèrent en général des milliers d'alertes chaque jour, ce qui dépasse largement le volume que les équipes de sécurité sont en mesure de traiter efficacement. Les alertes proviennent de nombreux outils déconnectés, laissant aux analystes de sécurité le soin de reconstituer le puzzle (voir figure 1-1).

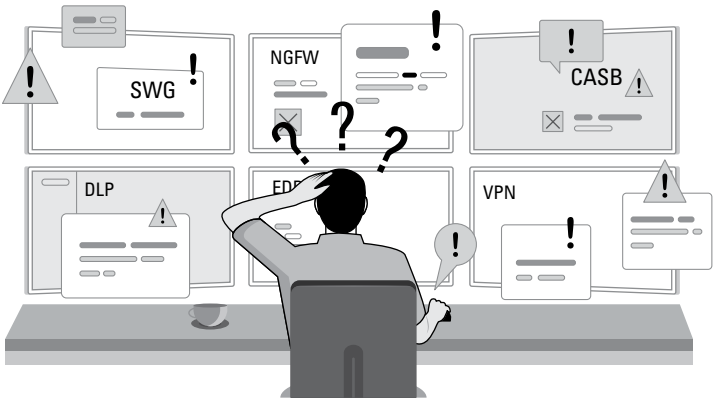

FIGURE 1-1 : Un trop grand nombre d'outils de sécurité entraîne une complexité et une lassitude concernant les alertes.

Pénurie de talents et de compétences en matière de cybersécurité

Au-delà de la fréquence et de la sophistication croissantes des menaces, et de la complexité et de la multiplication des outils de sécurité utilisés dans les entreprises, les défis du paysage moderne de la sécurité sont exacerbés par la pénurie mondiale de talents et de compétences en matière de cybersécurité. L'ISACA (Information Systems Audit and Control Association) estime que près des deux tiers des équipes de sécurité des entreprises manquent de personnel et que plus de la moitié d'entre elles ont des postes à pourvoir. Le Consortium international de certification en sécurité des systèmes d'information (ISC)[2] a estimé la pénurie mondiale de professionnels de la cybersécurité à 2,72 millions en 2021.

Comprendre la nécessité du changement

Outre l'évolution rapide du paysage des menaces et de la sécurité, les changements dans la nature du travail et dans les lieux et méthodes d'accès aux applications et aux données, nécessitent une modification fondamentale de la notion de confiance et de la manière dont nous accordons aux utilisateurs et aux appareils l'accès à nos applications et à nos données.

Évolution du travail, qui est passé d'un lieu où l'on se rend à une activité que l'on exerce

La nature du travail a changé : d'un lieu où les travailleurs se rendent, il est devenu une activité qu'ils exercent. Nous n'allons plus « au travail », mais nous « travaillons » tout simplement. Pour de nombreuses entreprises, la localisation de leurs collaborateurs et le lieu d'exécution de leurs tâches individuelles n'ont plus guère d'importance. Nous sommes désormais en mesure d'exercer nos activités quand et où nous le voulons. Ce changement est motivé par deux tendances majeures :

- **Les applications sont partout.** La plupart des entreprises sont passées à un modèle où l'on ne consomme plus des applications qui s'exécutent dans un data center d'entreprise. Le modèle de livraison des applications, y compris les logiciels en tant que service (SaaS), le web et le cloud, est désormais hybride. L'écrasante majorité des entreprises utilisent aujourd'hui une combinaison d'infrastructures cloud privées et publiques, de connexion Internet et de logiciels SaaS.

  
  CONSEIL

  Selon le *rapport* Flexera *2021 sur l'état du cloud*, 80 % des entreprises ont une stratégie de cloud hybride. Statista rapporte que l'organisation moyenne utilise 110 applications SaaS.

- **Les utilisateurs sont partout.** Aujourd'hui, de nombreuses organisations ont adopté un modèle de travail hybride, qui permet de travailler *à distance en partie* (à partir d'un bureau à domicile deux ou trois jours par semaine), en totalité ou entre les deux. Cette tendance s'est fortement accélérée en raison de la pandémie et, à mesure que les entreprises ont pris conscience des avantages en termes de productivité et de moral de leurs employés, elle est devenue la nouvelle norme au travail.

  
  CONSEIL

  Selon le rapport *The State of Hybrid Workforce Security 2021* de Palo Alto Networks, 76 % des employés veulent un modèle hybride, même après la pandémie.

Or, ce changement a des ramifications importantes pour l'informatique et la sécurité.

Auparavant, les entreprises connectaient leur personnel distant à des data centers et protégeaient l'accès aux applications hebergées dans ceux-ci et à toutes les applications web et SaaS. Pour ce faire, divers outils de sécurité ponctuels ont été déployés sur le périmètre du data center : pare-feu, proxys, systèmes de prévention des intrusions (IPS), passerelles d'accès cloud sécurisé (CASB), protection anti-malware, sécurité du système de noms de domaine (DNS), etc.

Dans ce modèle, les entreprises créaient leurs réseaux étendus (WAN) à l'aide de la commutation multiprotocole par étiquette (MPLS) et d'autres liaisons spécialisées reliant les sites distants au data center. Tout le trafic Internet était acheminé via le data center, ce qui signifiait que cette pile de sécurité massive pouvait être centralisée et que tout le trafic y transitait (voir la figure 1-2).

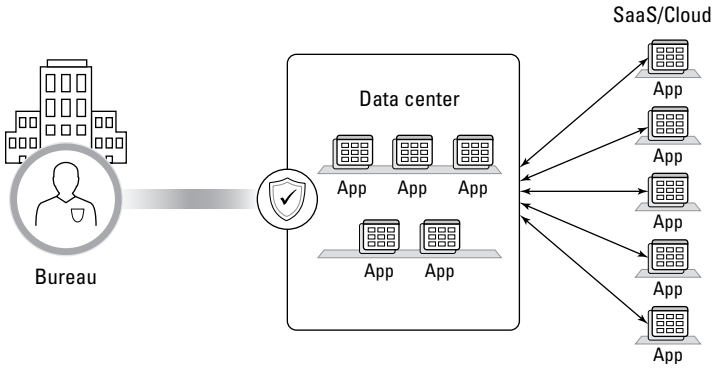

FIGURE 1-2 : La sécurité était relativement simple lorsque le travail était un endroit où l'on se rendait tous les jours.

Ce que nous voyons maintenant est un modèle complètement différent.

Des utilisateurs, des applications et des données partout

Les entreprises ont modifié leur architecture WAN, qui reliait auparavant les effectifs distants aux data centers, pour se connecter désormais directement à l'Internet. Par conséquent, elles doivent maintenant se concentrer sur la fourniture d'un accès sécurisé et fiable aux utilisateurs travaillant de n'importe où (depuis les bureaux

de l'entreprise et les sites distants, à domicile et sur des appareils mobiles) et se connectant à des applications et des données situées partout (dans des data centers, des clouds privés, des clouds publics et des applications SaaS).

Désormais, les utilisateurs se connectent directement à toutes les applications nécessaires pour effectuer leur travail (voir figure 1-3). L'emplacement de l'application importe moins ; ce qui compte désormais, c'est d'offrir une expérience homogène, optimisée et sécurisée pour accéder à toutes ces applications.

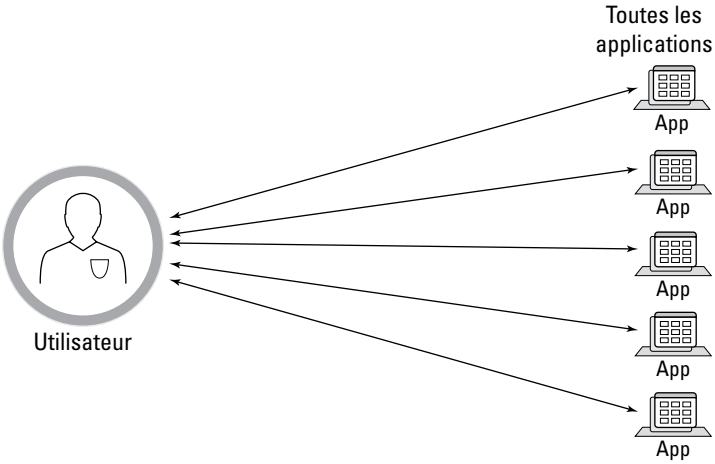

FIGURE 1-3 : Les utilisateurs se connectent désormais directement à leurs applications.

La connectivité directe aux applications augmente de façon exponentielle votre surface d'attaque

Cette connectivité directe aux applications constitue un changement radical par rapport au modèle traditionnel et augmente de façon exponentielle la surface d'attaque des entreprises. Plus la surface d'attaque s'étend, plus vous avez besoin de contrôles de sécurité et des accès pour protéger les applications et les données de l'entreprise (voir la figure 1-4).

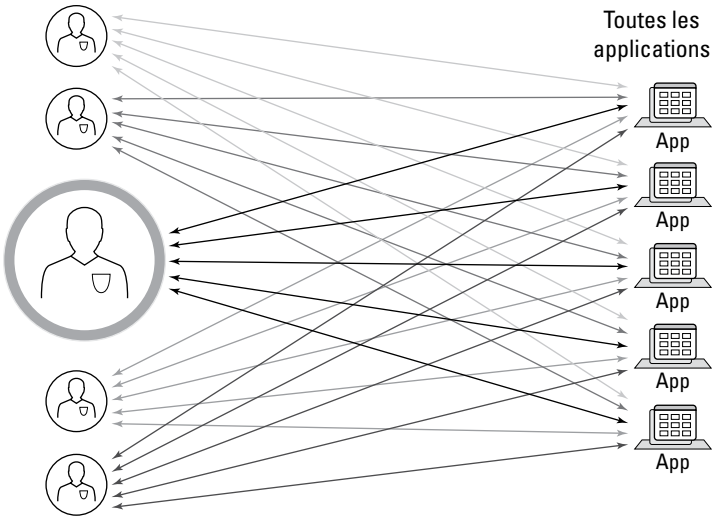

FIGURE 1-4 : La surface d'attaque a explosé.

Les VPN sont trop généraux

Les réseaux privés virtuels (VPN) ont été conçus pour permettre l'accès à un réseau local (LAN) ou à un sous-réseau au sein du LAN, en offrant un tunnel privé et chiffré permettant aux employés distants de se connecter au réseau de l'entreprise. Bien que cela puisse sembler être une solution pratique, les VPN n'ont malheureusement pas la flexibilité et la granularité nécessaires pour contrôler et voir exactement ce que les utilisateurs peuvent faire et à quelles applications ils peuvent accéder. Une fois que l'accès lui a été accordé, un utilisateur peut accéder à tout ce qui se trouve sur le réseau ou le sous-réseau, ce qui entraîne des failles de sécurité et des problèmes d'application des stratégies.

Le ZTNA, quant à lui, fournit un accès distant sécurisé aux applications sur la base de stratégies de contrôle d'accès granulaires. Il n'offre aux utilisateurs qu'un accès aux applications autorisées, au lieu d'adopter une approche d'accès universel sur vérification, telle qu'utilisée par les VPN. Ainsi, le ZTNA fournit une approche basée sur le principe du moindre privilège pour réduire considérablement la surface d'attaque et améliorer la posture de sécurité globale.

Qu'est-ce que l'accès réseau Zero Trust ?

Le ZTNA est une catégorie de produits qui fournit un accès distant sécurisé aux applications et aux services sur la base de stratégies de contrôle d'accès définies. Par défaut, les solutions ZTNA refusent l'accès, en ne donnant à l'utilisateur que l'accès à une application ou à un service qui lui a été explicitement accordé. Il est important de comprendre les lacunes en matière de sécurité et les avantages des solutions ZTNA pour les entreprises, car de plus en plus d'utilisateurs distants rejoignent le réseau.

RAPPEL

Le ZTNA est un élément clé de la philosophie « ne jamais faire confiance, toujours vérifier », développée par Forrester pour identifier le besoin de protéger les données. Le ZTNA exige des utilisateurs de s'authentifier auprès d'une passerelle avant d'obtenir l'accès aux outils dont ils ont besoin. Cette exigence permet d'identifier les utilisateurs et de créer des politiques pour limiter l'accès, minimiser les pertes de données et remédier rapidement aux éventuels problèmes ou menaces.

Les bases du ZTNA

Avec le ZTNA, l'accès est établi après que l'utilisateur a été authentifié par la passerelle d'accès. Le service ZTNA fournit alors l'accès à l'application pour l'utilisateur par le biais d'un tunnel sécurisé et chiffré. Cela permet de renforcer la protection des applications et des services de l'entreprise, en protégeant les adresses de protocole Internet (IP) qui seraient autrement visibles dans le domaine public.

À l'instar des périmètres définis par logiciel (SDP), le ZTNA exploite le concept de « dark cloud » empêchant les utilisateurs de voir les applications et les services auxquels ils ne sont pas autorisés à accéder. Cela protège des mouvements latéraux, lorsqu'un terminal ou des identifiants compromis permettraient à un pirate d'effectuer un balayage et de se tourner vers d'autres services.

Le ZTNA 1.0

Les solutions ZTNA initiales, ou ZTNA 1.0, ont été introduites à une époque où le paysage des menaces, les réseaux d'entreprise et les méthodes de travail étaient très différents de ce qu'ils sont aujourd'hui. Par conséquent, les solutions ZTNA 1.0 ne sont plus adaptées au nouveau monde du travail, et les attaquants trouvent de nouveaux moyens d'exploiter les limites de ces approches.

Le ZTNA 1.0 a été conçu pour protéger les organisations en limitant leur exposition et en réduisant leur surface d'attaque. Il s'appuie sur une passerelle d'accès pour faciliter la connectivité à une application. Lorsqu'un utilisateur demande l'accès à une application, cette passerelle détermine si l'utilisateur doit avoir l'autorisation d'accéder à une application. Après vérification de l'autorisation, la passerelle accorde l'accès et la connexion est établie (voir figure 1-5).

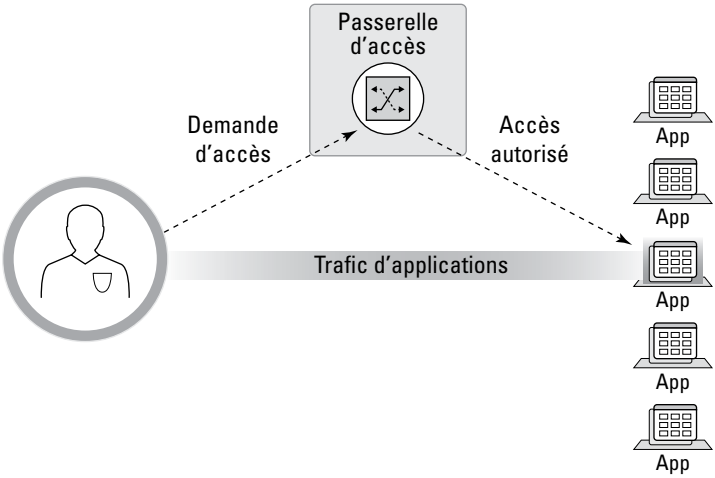

FIGURE 1-5 : Le secteur a tenté de résoudre le problème de l'accès sécurisé avec le ZTNA 1.0.

Et voilà ! La passerelle n'intervient plus, et l'utilisateur bénéficie désormais d'un accès complet à l'application sans aucune surveillance supplémentaire de la part du système de sécurité.

Cette approche « d'autorisation et d'exclusion » constitue le modèle architectural du ZTNA 1.0. Ce modèle n'est pas seulement problématique dans le contexte du paysage actuel des menaces ; il est dangereux.

Le ZTNA 1.0 présente des limites majeures dans l'environnement actuel

Un grand nombre de solutions ZTNA 1.0 sont basées sur des architectures SDP. Ces dernières ne fournissent aucune inspection du contenu, créant ainsi une divergence entre les types de protection disponibles pour chaque application. En termes de protection homogène, il appartient à l'organisation d'intégrer des contrôles supplémentaires au modèle ZTNA et d'instaurer une inspection de tout le trafic dans toutes les applications. Au-delà de ces défis, cinq problématiques majeures limitent l'efficacité des solutions ZTNA 1.0 dans l'environnement de sécurité et de travail actuels en évolution rapide.

Viole le principe du moindre privilège

Le principe du moindre privilège exige qu'un utilisateur ne se voie accorder que le niveau minimum d'accès à une application ou à une ressource nécessaire pour effectuer une tâche autorisée, et rien d'autre. Selon la stratégie Zero Trust, toute tentative de connexion à une application ou à une ressource du réseau – y compris les utilisateurs, les applications et les appareils – n'est jamais intrinsèquement fiable.

Les solutions ZTNA 1.0 existantes gèrent l'accès aux applications au niveau des couches 3 (réseau) et 4 (transport) du modèle OSI (Open Systems Interconnection) en utilisant uniquement l'adresse IP et les ports TCP (Transmission Control Protocol) et UDP (User Datagram Protocol).

Un réseau n'est pas identique à une application, mais les solutions ZTNA 1.0 s'appuient sur des contrôles d'accès au niveau du réseau pour fournir aux utilisateurs un accès au niveau de l'application. Malheureusement, le fait de s'appuyer sur des stratégies définies aux niveaux 3 et 4 engendre un certain nombre de problèmes. Par exemple, si une application utilise des ports ou des adresses IP dynamiques, vous devez accorder l'accès à de larges plages d'adresses IP et de ports, exposant ainsi plus de surface que nécessaire. Impossible par ailleurs de limiter l'accès au niveau de la sous-application ou de la fonction de l'application ; l'accès ne peut être accordé qu'à des applications entières. Résultat : les utilisateurs se retrouvent avec beaucoup plus d'accès que ce qui est souhaité ou prévu (voir la figure 1-6).

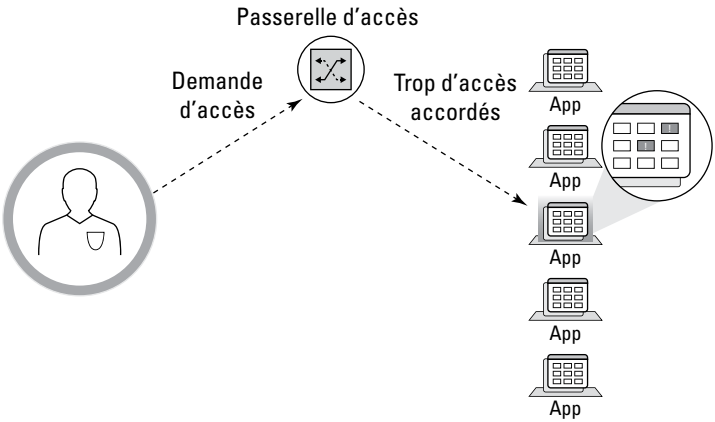

FIGURE 1-6 : Le ZTNA 1.0 viole le principe du moindre privilège.

ATTENTION

Un malware qui écoute sur les mêmes adresses IP et numéros de port que les applications autorisées peut communiquer librement avec l'infrastructure de commande et contrôle (C2) et se propager latéralement.

Intègre un modèle d'autorisation et d'exclusion

Autre limite des solutions ZTNA 1.0 : elles reposent sur un modèle risqué d'autorisation et d'exclusion (voir la figure 1-7). Lorsque la passerelle d'accès établit la connexion entre l'utilisateur et l'application, le trafic de l'utilisateur et de l'appareil est fiable et aucune autre vérification n'est effectuée pendant la durée de la session.

Supposer que la confiance ne doit être vérifiée qu'une seule fois et qu'elle ne doit plus jamais l'être est synonyme de désastre. Bien des choses peuvent se produire après que la confiance a été établie. Le comportement des utilisateurs et des applications peut changer, et les applications peuvent être compromises.

ATTENTION

De nombreuses menaces modernes s'appuient sur et profitent d' activités autorisées pour éviter de déclencher des alarmes.

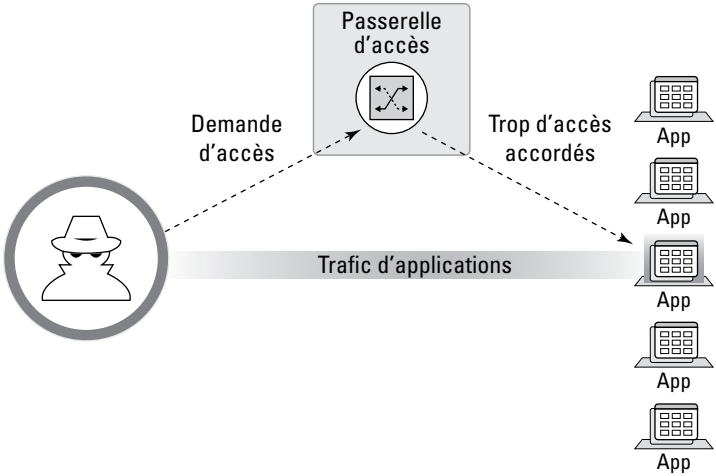

FIGURE 1-7 : Le ZTNA 1.0 autorise et exclut.

Ne fournit pas d'inspection de sécurité

Les solutions ZTNA 1.0 n'inspectent pas non plus le trafic des applications (voir la figure 1-8). Lorsqu'une connexion est établie, le ZTNA 1.0 fait implicitement confiance à cette session active et n'effectue donc aucune inspection supplémentaire du trafic. Si le terminal est compromis et qu'un malware est introduit dans la session, une solution ZTNA 1.0 n'a aucun moyen de détecter le trafic malveillant, ou tout autre trafic compromis, et de réagir en conséquence.

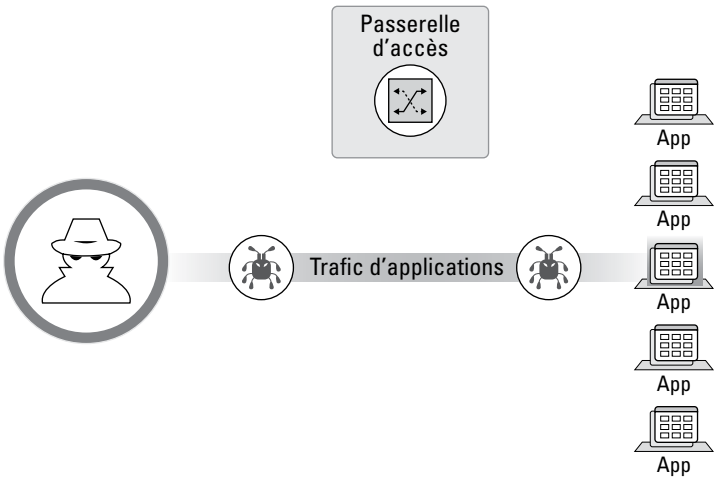

FIGURE 1-8 : Le ZTNA 1.0 ne fournit aucune inspection de sécurité.

Ne protège pas les données

Les solutions ZTNA 1.0 n'assurent pas la protection des données, en particulier celles contenues dans des applications privées (voir la figure 1-9). Cela laisse une bonne partie du trafic de l'organisation vulnérable à l'exfiltration de données par des personnes internes malveillantes ou des attaquants externes. De plus, cette approche nécessite des solutions supplémentaires de prévention des pertes de données (DLP) pour protéger les données sensibles dans les applications privées par rapport aux applications SaaS. Le ZTNA 1.0 introduit plus de complexité et de risques, car il exige des organisations qu'elles utilisent des produits à points multiples pour sécuriser les données partout.

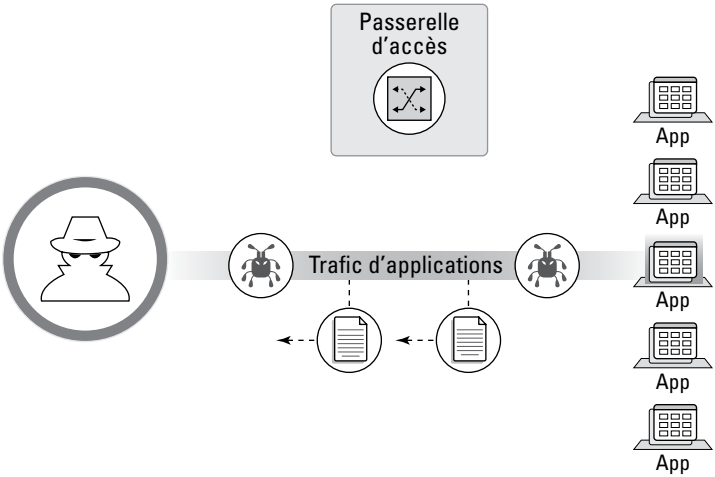

FIGURE 1-9 : Le ZTNA 1.0 ne fournit aucune protection des données.

Ne sécurise pas toutes les applications

Enfin, les solutions ZTNA 1.0 ne permettent pas de couvrir toutes les applications (voir la figure 1-10). Elles ne prennent en charge ni les applications cloud ni les applications qui utilisent des ports dynamiques ni les applications initiées par le serveur – comme les applications d'assistance technique qui utilisent des connexions initiées par le serveur pour les périphériques distants. Les solutions ZTNA 1.0 sont également incompatibles avec les applications SaaS.

Les piles d'applications cloud-native modernes sont composées de nombreux containers et microservices qui utilisent souvent des adresses IP et des numéros de port dynamiques. Le contrôle d'accès

ZTNA 1.0 est totalement inefficace dans ces environnements, car il nécessite l'ouverture de l'accès à de larges plages d'adresses IP et de ports, ce qui va à l'encontre du principe du Zero Trust.

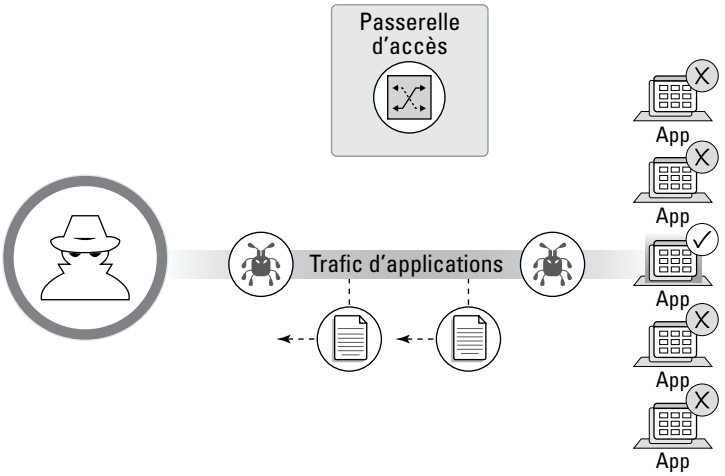

FIGURE 1-10 : Le ZTNA 1.0 ne peut pas sécuriser toutes les applications.

Alors qu'un nombre croissant d'organisations adoptent le cloud et mènent leurs activités par le biais d'applications cloud-native, le ZTNA 1.0 devient de plus en plus obsolète.

CONSEIL

Avec autant de limites dans le ZTNA 1.0, il y a de quoi se demander comment ce concept a-t-il bien pu arriver sur le marché ? Rappelez-vous, le ZTNA 1.0 a été lancé il y a une dizaine d'années. Depuis, le monde a changé. Avant le ZTNA 1.0, l'accès VPN était vraiment suffisant, car toutes vos applications étaient situées dans le data center local et la plupart des utilisateurs travaillaient au bureau. Le ZTNA 1.0 a été introduit pour résoudre certains des problèmes associés aux VPN lorsque les utilisateurs et les applications ont commencé à se déplacer en dehors des bureaux et des data centers des entreprises. Aujourd'hui, dans un monde où les environnements réseau et les effectifs sont hybrides – où le travail est désormais une activité et non plus un lieu, et où les applications et les utilisateurs sont partout – une nouvelle approche s'impose. Le chapitre 2 explique comment le ZTNA 2.0 relève les défis actuels en matière de sécurité et va au-delà des limites du ZTNA 1.0.

DANS CE CHAPITRE

- Implémenter un accès avec le minimum de privilèges
- Assurer une vérification en continu de la confiance
- Permettre une inspection en continu de la sécurité
- Sécuriser toutes les données
- Contrôler et protéger l'accès aux applications

Chapitre 2
Présentation de l'accès réseau Zero Trust 2.0

Les approches traditionnelles en matière d'accès à distance sécurisé et les architectures obsolètes – comme les réseaux privés virtuels (VPN) et la version initiale de l'accès réseau Zero Trust (ZTNA) – ne sont pas en mesure de faire face à l'assaut des nouvelles cyberattaques toujours plus sophistiquées sur nos surfaces d'attaque qui explosent. Il est clair qu'une nouvelle approche s'impose. Ce chapitre présente le ZTNA 2.0 et explique comment il relève les défis de sécurité actuels tout en surmontant les limites des anciennes approches afin de permettre un accès distant sécurisé pour le personnel hybride d'aujourd'hui.

Accorder pleinement l'accès avec le minimum de privilèges

Le ZTNA 2.0 utilise des capacités d'identification avec état des applications, des utilisateurs et des appareils pour permettre un accès avec le minimum de privilèges (voir figure 2-1).

Cela signifie comprendre les applications d'un point de vue fondamental sur la couche 7 (application) du modèle OSI (Open Systems Interconnection) – au-delà des constructions réseau de bas niveau

telles que la couche 3 (réseau [adresse IP]) et la couche 4 (transport [port ou protocole]) – en recueillant en permanence des informations sur la session TCP (Transmission Control Protocol), les liaisons d'applications, le comportement des applications, les protocoles avec état, etc.

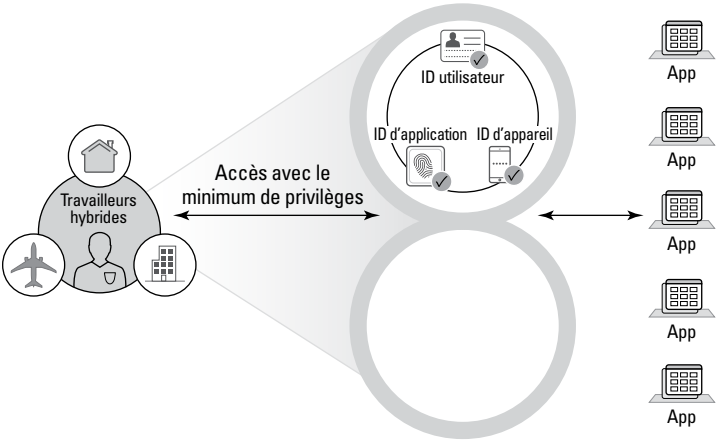

FIGURE 2-1 : Le ZTNA 2.0 utilise l'identification des applications, des utilisateurs et des appareils pour garantir un accès avec le minimum de privilèges.

Ce niveau de visibilité sur les applications, en particulier les applications modernes à microservices, permet au ZTNA 2.0 de fournir des contrôles précis pour empêcher l'exposition de fonctions de sous-applications ou d'autres schémas de communication auxquels les utilisateurs n'ont pas besoin d'accéder. Dans le même temps, les contrôles d'identification recueillent en permanence des informations sur les utilisateurs et leurs appareils. En combinant l'identification des applications, des utilisateurs et des appareils, vous allez au-delà des simples assurances de confiance ponctuelles (comme dans le cas du ZTNA 1.0) : vous disposez d'un environnement offrant des informations contextuelles riches pour prendre de meilleures décisions en matière de contrôle des accès. Avec le ZTNA 2.0, les entreprises peuvent permettre à tout utilisateur, sur tout appareil, d'accéder à l'application spécifique qu'il demande et recueillir en permanence des informations supplémentaires pour réagir aux changements en temps réel, ce qui réduit considérablement la surface d'attaque tout en imposant un véritable accès avec le minimum de privilèges.

Assurer la vérification en continu de la confiance

Le principe fondamental du Zero Trust consiste à supprimer la confiance implicite. Autrement dit, il s'agit de « ne jamais faire confiance, toujours vérifier ». Or, sans une capacité de vérification en continu de la confiance, le système doit supposer que l'utilisateur, l'appareil et l'application se comportent tous de manière digne de confiance, indéfiniment, lorsqu'une connexion est établie. Mais bien des choses peuvent se produire pour compromettre la fiabilité une fois l'accès octroyé, notamment des changements dans le comportement de l'utilisateur, de l'appareil ou de l'application, ou une compromission de la sécurité.

La vérification en continu de la confiance réalisée par le ZTNA 2.0 permet de surveiller en permanence la posture des appareils et toute modification de celle-ci, ainsi que les comportements des utilisateurs et des applications, afin de réagir en temps réel, si nécessaire (voir la figure 2-2).

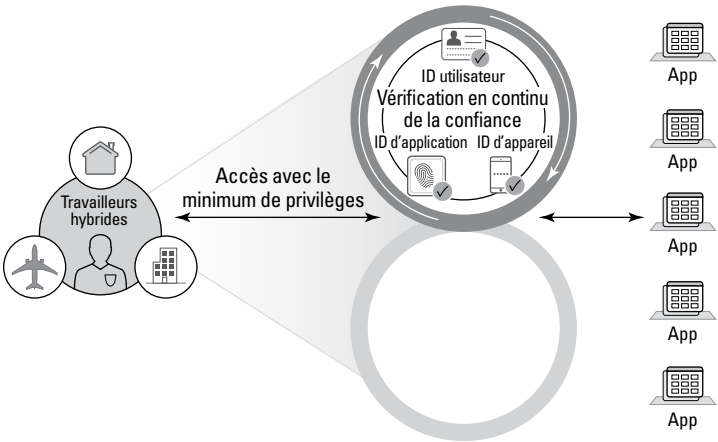

FIGURE 2-2 : La vérification en continu de la confiance permet de surveiller en permanence la posture des appareils, le comportement des applications et celui des utilisateurs, même après leur accès aux applications.

Assurer une inspection en continu de la sécurité

Le ZTNA 2.0 fournit une inspection en continu de la sécurité avec renseignements sur les menaces, filtrage avancé des URL (Uniform Resource Locator), prévention des menaces, sécurité des logiciels en tant que service (SaaS), sécurité du système de noms de domaine (DNS), etc. Les capacités d'inspection approfondie des paquets (DPI) et d'inspection en continu de la sécurité s'appuient également sur des technologies de prévention des menaces alimentées par l'intelligence artificielle (IA) et le machine learning (ML) pour stopper les attaques « zero day » en ligne (voir figure 2-3).

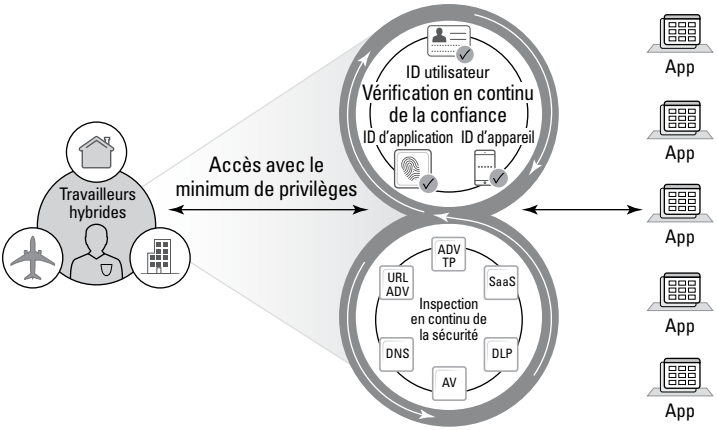

FIGURE 2-3 : L'inspection en continu de la sécurité surveille votre environnement pour le protéger des menaces.

Protéger toutes les données

Le ZTNA 2.0 applique de manière homogène des capacités avancées de prévention des pertes de données (DLP) à toutes les données des applications. Les mêmes stratégies DLP sont appliquées (que les données se trouvent dans une application personnalisée, une application SaaS, une application web, un référentiel public ou une base de données), ce qui évite d'avoir à deviner quelles applications sont protégées et quelles données sont sécurisées. Les organisations peuvent mettre en place de solides stratégies de protection des données et de sécurité pour l'ensemble de leurs applications à partir d'une solution unique (voir la figure 2-4).

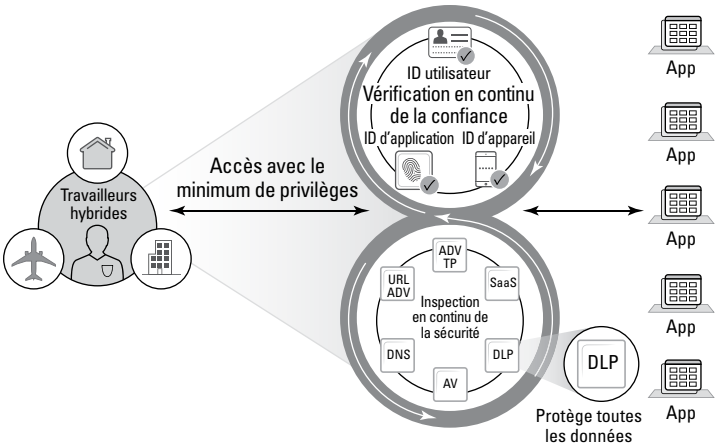

FIGURE 2-4 : La protection homogène des données applique les mêmes stratégies robustes de protection et de sécurité des données dans tout votre environnement.

Sécuriser toutes les applications

Le ZTNA 2.0 assure une sécurité homogène pour toutes les applications de votre organisation. Il peut s'agir d'une application cloud-native moderne basée sur des microservices qui n'est pas limitée par des adresses IP et des ports, d'une application SaaS, d'une application personnalisée ou d'une application héritée (voir la figure 2-5).

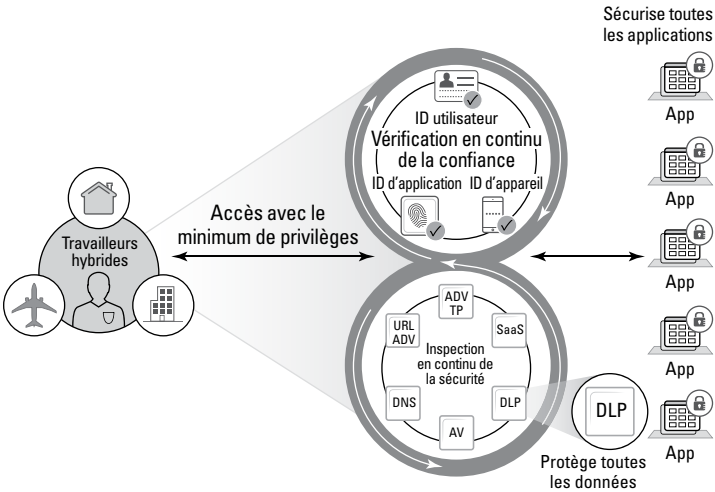

FIGURE 2-5 : Le ZTNA 2.0 assure une sécurité homogène pour toutes vos applications, qu'elles soient cloud-native, SaaS, personnalisées ou héritées.

RAPPEL

Le ZTNA 2.0 surmonte les limites des solutions ZTNA 1.0 et fournit de meilleurs résultats en matière de sécurité pour soutenir la transformation numérique et les besoins en effectifs hybrides auxquels les organisations sont actuellement confrontées. Les cinq principes clés du ZTNA sont les suivants :

- **Moindre privilège :** utilise l'application la plus stricte du principe du moindre privilège, en fournissant un contrôle d'accès de la couche 3 (réseau) à la couche 7 (application) pour réduire considérablement la surface d'attaque.
- **Vérification en continu de la confiance :** lorsque le comportement d'un utilisateur, d'une application ou d'un appareil change, il faut évaluer en permanence le niveau de confiance accordé et la capacité à répondre de manière appropriée (en temps réel) à tous les changements.
- **Inspection en continu de la sécurité :** l'ensemble du trafic est surveillé en permanence pour assurer une protection contre toutes les menaces, y compris les menaces avancées persistantes (APT) et les attaques « zero day », ainsi que tous les vecteurs de menace.
- **Protection des données :** toutes les données sont protégées grâce à des stratégies appliquées de manière homogène à l'ensemble des données applicatives, depuis les données des applications fonctionnant sur des mainframes hérités jusqu'aux données stockées dans des applications modernes, cloud-native et collaboratives.
- **Sécurité homogène pour toutes les applications :** toutes les applications de l'entreprise, y compris les applications personnalisées, les applications cloud-native et les applications SaaS, sont protégées et sécurisées.

DANS CE CHAPITRE

- Reconnaître l'importance d'une expérience utilisateur exceptionnelle
- Fournir une solution simple et unifiée

Chapitre 3
Comprendre les capacités essentielles à la réussite du ZTNA 2.0

Ce chapitre explique pourquoi il est essentiel d'offrir une expérience utilisateur exceptionnelle et une solution unifiée pour réussir l'adoption de votre solution ZTNA 2.0.

Offrir une expérience utilisateur exceptionnelle

Si vous demandez à vos utilisateurs ce qu'ils pensent des outils de sécurité de votre organisation, vous n'entendrez probablement pas : « J'adore l'expérience utilisateur ! ». Au contraire, les outils de sécurité sont notoirement difficiles à comprendre et à utiliser pour les utilisateurs, et ils les ralentissent la plupart du temps. L'analyse antimalware prive vos utilisateurs d'une capacité mémoire précieuse et ralentit leur ordinateur. La connexion au réseau privé virtuel (VPN) ralentit leur accès à Internet et augmente la latence de leurs applications. Par conséquent, nombre d'entre eux trouvent des moyens créatifs de contourner les contrôles de sécurité qui sont censés les protéger d'eux-mêmes.

Les solutions ZTNA 1.0 actuelles ne sont pas différentes. Elles s'appuient sur des appareils physiques déployés dans des installations de colocation et assemblés de façon peu cohérente, en utilisant l'Internet public comme dorsale principale. Cette approche limite considérablement la portée, l'échelle et les performances de la solution tout en imposant une dépendance indésirable à des data centers tiers et à des connexions non optimales. Ces solutions n'offrent pas non plus de véritable architecture mutualisée pour pallier les problèmes de « voisins bruyants » et de « partage du sort », ce qui oblige les clients à sacrifier la sécurité pour l'expérience.

Pour garantir des performances élevées et constantes, les solutions ZTNA 2.0 doivent fournir un plan de données dédié à chaque client, évitant ainsi le problème du « voisin bruyant » des approches ZTNA 1.0.

Les solutions ZTNA 2.0 doivent également être conçues avec des capacités natives de surveillance de l'expérience numérique (DEM). Elles peuvent ainsi identifier proactivement les problèmes et contribuer à les résoudre automatiquement pour réduire le nombre de tickets gérés par les administrateurs informatiques. À la clé : une meilleure compréhension et une meilleure visibilité pour une expérience de qualité exceptionnelle.

JARGON TECHNIQUE

Selon Gartner, « le contrôle de l'expérience numérique (DEM) est une discipline d'analyse des performances qui prend en charge l'optimisation de l'expérience opérationnelle et du comportement d'un agent numérique, humain ou machine, avec le portefeuille d'applications et de services des entreprises. Ces utilisateurs, physiques ou virtuels, peuvent être un mélange d'utilisateurs externes situés à l'extérieur et à l'intérieur du périmètre du pare-feu. Cette discipline cherche également à observer et à modéliser le comportement des utilisateurs comme un flux d'interactions sous la forme d'un parcours client ».

Fournir une solution unifiée

Les solutions ZTNA 1.0 vous obligent à gérer des stratégies distinctes sur différentes consoles de gestion pour sécuriser complètement tous les utilisateurs et toutes les applications. Avec le ZTNA 1.0, il est impossible d'éviter efficacement les incidents ou de les détecter et d'y répondre lorsque la gestion, les stratégies et les données sont dispersées dans votre infrastructure.

Les solutions ZTNA 2.0 assurent une sécurité supérieure tout en offrant des performances sans compromis et une expérience utilisateur exceptionnelle, le tout autour d'une seule approche unifiée. Le ZTNA 2.0 offre une architecture véritablement cloud-native, conçue pour sécuriser les entreprises numériques d'aujourd'hui à l'échelle du cloud, en fournissant des performances sans compromis soutenues par des contrats de niveau de service (SLA) sur le temps de fonctionnement et les performances qui garantissent des expériences exceptionnelles aux utilisateurs.

Entièrement logiciel et neutre sur le plan matériel, le ZTNA 2.0 assure une mise à l'échelle automatique pour s'adapter à l'évolution des effectifs hybrides et aux demandes changeantes des entreprises sans nécessiter d'interactions ou de processus manuels.

RAPPEL

Les solutions ZTNA 2.0 offrent un produit unifié pour toutes les fonctionnalités, notamment des solutions ZTNA, SWG, CASB, FWaaS, DLP de nouvelle génération et bien d'autres encore.

ZTNA ET SASE

Le périmètre de service d'accès sécurisé (SASE) est la convergence des services de réseau étendu (WAN) et de sécurité dans un « périmètre » de services fournis dans le cloud. Il a été conçu pour aider les organisations à moderniser leurs infrastructures réseau et de sécurité afin de répondre aux besoins des environnements et des effectifs hybrides.

Les solutions SASE regroupent plusieurs produits ponctuels – accès réseau Zero Trust (ZTNA), passerelle web sécurisée (SWG) dans le cloud, passerelle d'accès cloud sécurisé (CASB), pare-feu en tant que service (FWaaS) et réseau étendu défini par logiciel (SD-WAN) – au sein d'un service intégré, ce qui réduit la complexité du réseau et de la sécurité tout en augmentant l'agilité organisationnelle.

DANS CE CHAPITRE

- Se débarrasser des réseaux privés virtuels existants
- Protéger les applications web et le trafic Internet
- Assurer la protection avancée des applications SaaS et la prévention des pertes de données

Chapitre 4
Comment prendre un bon départ avec le ZTNA 2.0

La mise en place de l'accès réseau Zero Trust (ZTNA) 2.0 ne devrait pas être une tâche difficile, et ne devrait pas nécessiter de compromis. Tout est une question d'alignement : il s'agit de mettre en correspondance les besoins de votre organisation avec les principales préoccupations ou les principaux défis auxquels vous êtes confrontés, et de résoudre ces défis sans que cela ne nécessite de changement ou de perturbation architecturale massive. Ce chapitre examine trois cas d'utilisation courants qui représentent certains des plus grands défis actuels des organisations.

Remplacement du VPN

Depuis des années, le réseau privé virtuel (VPN) sert d'outil standard pour connecter les utilisateurs distants à un réseau d'entreprise. Les VPN ont été principalement conçus pour permettre aux utilisateurs distants d'accéder en toute sécurité aux ressources réseau de l'entreprise. Cependant, les applications et les charges de travail étant de plus en plus souvent transférées dans le cloud, les organisations n'ont pas seulement besoin d'un accès à distance – il leur faut également un accès sécurisé aux applications cloud et à l'Internet.

Les VPN traditionnels utilisent une architecture en étoile (voir figure 4-1) pour connecter des sites distants (branches) à un bureau central ou à un data center (hub). Cette connectivité d'emplacement à emplacement est l'architecture optimale pour les applications de data center, car l'objectif est d'atteindre le « hub » où sont situées vos applications et données internes.

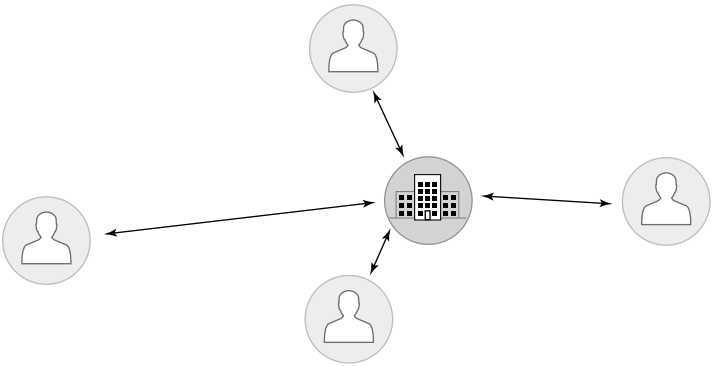

FIGURE 4-1 : Architecture VPN classique en étoile.

Ce modèle échoue quand on fait intervenir un mélange d'applications cloud et Internet. Avec des VPN traditionnels, le trafic se dirige en premier vers la passerelle ou le concentrateur du VPN, même si l'application est hébergée dans le cloud (voir la figure 4-2). Par conséquent, le trafic va vers la passerelle VPN du siège ou du data center de l'entreprise, puis sort du pare-feu du périmètre pour aller sur Internet, la réponse de l'application retournant au siège ou au data center avant de revenir à l'utilisateur. Avec des applications cloud, ce trafic suit essentiellement un chemin en « trombone », ce qui allonge et ralentit le parcours pour atteindre un lieu accessible par Internet. Cela est judicieux du point de vue de la sécurité, mais n'a pas de sens pour l'optimisation du réseau.

JARGON TECHNIQUE

Le *tromboning* est une pratique consistant à acheminer le trafic réseau via un point de contrôle (comme un pare-feu). Il s'agit souvent de renvoyer le trafic destiné à l'Internet, par exemple, à travers un réseau MPLS (Multiprotocol Label Switching) d'entreprise et un pare-feu central plutôt que par une route plus directe. Autre inconvénient du tromboning : il augmente la latence et la complexité du réseau.

L'utilisation d'applications cloud par l'intermédiaire d'anciens VPN a un impact négatif sur l'expérience des utilisateurs. Par conséquent, ces derniers évitent autant que possible d'utiliser les VPN. Ils ont

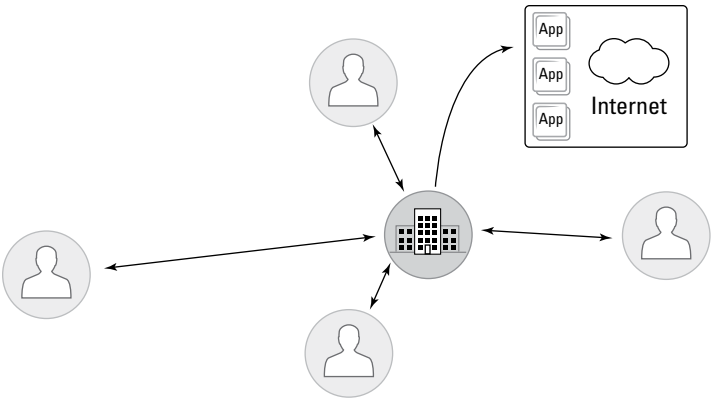

FIGURE 4-2 : Les VPN traditionnels acheminent le trafic vers le cloud.

tendance à s'y connecter s'ils doivent accéder au data center interne et à se déconnecter s'ils n'en ont pas besoin, ce qui engendre de multiples problèmes. Quand les utilisateurs ne sont pas connectés, leur organisation perd la visibilité sur l'utilisation des applications, le contrôle sur l'accès à des applications non validées et la capacité à faire appliquer les stratégies de sécurité.

L'une des priorités pour de nombreuses organisations consiste aujourd'hui à remplacer les technologies VPN obsolètes qui offrent une granularité insuffisante des contrôles, des performances médiocres et une expérience utilisateur insatisfaisante. Les initiatives de remplacement des VPN sont généralement motivées par plusieurs facteurs, notamment :

- **Les applications évoluent vers un véritable modèle hybride, tirant parti des environnements sur site, dans le cloud et multicloud :** les technologies VPN traditionnelles qui acheminent le trafic vers un « concentrateur » sur site ne sont pas évolutives et ne permettent pas d'offrir la meilleure expérience utilisateur possible.
- **Les exigences d'accès aux applications d'entreprise changent :** traditionnellement, les employés utilisaient des appareils gérés pour effectuer des tâches professionnelles. Or, de plus en plus d'appareils non gérés, comme les smartphones personnels et les tablettes, se sont introduits dans les réseaux d'entreprise et peuvent accéder aux applications de l'entreprise.

- **Les organisations sont à la recherche d'un modèle homogène et universel de protection et de sécurité pour toutes les applications, et pas seulement pour les applications web ou existantes.**

Les technologies VPN n'ont pas été conçues pour assurer l'évolution rapide, les hautes performances et la fourniture constante de services de sécurité avancés nécessaires pour connecter des effectifs hybrides à l'ensemble des applications dont ils ont besoin pour accomplir leur travail. C'est ainsi que les organisations ont commencé à remplacer les déploiements VPN obsolètes par des solutions ZTNA.

Plusieurs solutions peuvent répondre à certains de ces besoins, mais seul le ZTNA 2.0 transforme le réseau et la sécurité pour prendre en charge les appareils gérés et non gérés, tout en assurant une protection homogène de toutes les applications dans toute l'entreprise.

En remplaçant votre VPN par une solution ZTNA 2.0, vous offrez un accès distant sécurisé aux applications situées dans le cloud public, le cloud privé et le data center à vos collaborateurs mobilesou à domicile ou sur un site distant (voir la figure 4-3). Les principales fonctionnalités comprennent la vérification de la confiance et l'inspection de la sécurité en continu pour fournir :

- Un modèle Zero Trust pour l'accès aux applications privées
- Une prise en charge de l'accès des clients gérés ou non
- Une protection homogène dans toute l'entreprise

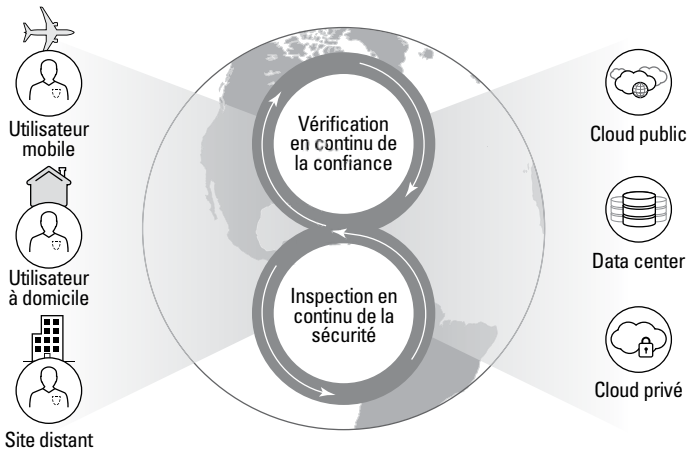

FIGURE 4-3 : Le ZTNA 2.0 en remplacement du VPN.

Les principaux avantages du ZTNA 2.0 pour les projets de remplacement du VPN sont les suivants :

- Meilleure expérience utilisateur
- Produit unifié
- Intégration du réseau étendu défini par logiciel (SD-WAN)

CONSEIL

Remplacez les anciennes technologies VPN par une solution moderne ZTNA 2.0 qui offre un accès réseau sécurisé aux travailleurs à distance et hybrides, résout les problèmes de performances et simplifie la gestion.

SÉCURISATION DE L'ACCÈS PRIVÉ POUR UNE SOCIÉTÉ DE CONSEIL FIGURANT AU CLASSEMENT FORTUNE 100

Une société de services de conseil classée au Fortune 100 recherchait une solution d'accès à distance moderne qui lui permettrait de mettre fin à son déploiement VPN multifournisseur vieillissant et non évolutif.

Compte tenu de la nature hétéroclite de sa solution VPN, la société avait du mal à homogénéiser la visibilité et la sécurité pour l'ensemble de ses employés et de ses sites répartis dans le monde.

En outre, le niveau de satisfaction des employés à l'égard des solutions en place était très faible. Ils étaient régulièrement confrontés à des connexions lentes, des performances irrégulières et des expériences utilisateur médiocres d'un site à l'autre et d'un emplacement à l'autre.

Objectifs du projet

- Mise hors service de la solution VPN d'accès à distance non évolutive.
- Visibilité et sécurité homogènes pour les employés, quel que soit l'endroit où ils se trouvent.
- Amélioration de l'expérience utilisateur.

Ce client avait besoin d'une solution de remplacement moderne pour son VPN et a choisi le ZTNA 2.0 proposé par Palo Alto Networks. Grâce au ZTNA 2.0, il est désormais en mesure de connecter de manière homogène ses 350 000 utilisateurs répartis dans 158 pays, tout en

(suite)

(suite)

fournissant à des centaines de sites distants dans le monde une connectivité directe et sécurisée à Internet. De plus, le ZTNA 2.0 garantit un accès homogène et sécurisé à toutes les applications, y compris les applications existantes, dans plus de 30 data centers et sites cloud.

Impact

- 350 000 utilisateurs sécurisés dans 158 pays
- Internet local avec la sécurité du cloud protégeant des centaines de bureaux dans le monde entier
- Solution ZTNA pour des milliers d'applications dans plus de 30 data centers et sites cloud

Sécuriser l'accès à Internet

Les organisations utilisent de nombreuses applications, certaines situées sur site et d'autres dans le cloud. À mesure que les entreprises et leurs effectifs mobiles et hybrides se développent, il devient de plus en plus difficile de protéger les utilisateurs distants des menaces lorsqu'ils accèdent à ces diverses applications.

Les applications sur site sont généralement accessibles via un VPN d'accès à distance. Cependant, lorsque les utilisateurs accèdent à des applications et des services sur Internet, ils sont déconnectés du VPN et exposés à des risques. Les organisations utilisent des passerelles web sécurisées (SWG) pour fournir un accès Internet sûr lorsque les utilisateurs distants sont déconnectés du VPN.

Une SWG agit généralement comme un *proxy* (intermédiaire) entre les utilisateurs et les ressources Internet afin de protéger les utilisateurs contre les menaces du web, en plus d'appliquer et de faire respecter les règles de bon usage de l'entreprise. Au lieu de se connecter directement à un site web, un utilisateur est dirigé vers la SWG, qui est alors chargée de connecter l'utilisateur au site web souhaité et d'exécuter des fonctions comme le filtrage des URL, la visibilité du web, l'inspection des contenus malveillants, les contrôles d'accès au web et d'autres mesures de sécurité.

RAPPEL

Les SWG permettent aux entreprises de :

- Bloquer l'accès à des sites web ou à des contenus inappropriés sur la base de règles de bon usage

- Appliquer des stratégies de sécurité pour rendre l'accès à Internet plus sûr
- Protéger les données contre les transferts non autorisés

Cependant, les anciennes SWG sont généralement déployées en tant qu'appliances sur les réseaux d'entreprise, ce qui exige que le trafic utilisateur soit réacheminé vers la SWG, qui est souvent située dans un data center d'entreprise. Cet acheminement inefficace du trafic augmente la latence et a un impact négatif sur l'expérience des utilisateurs.

Autre défi des anciennes SWG : il s'agit typiquement de solutions autonomes qui n'ont pas la capacité de coordonner les flux de travail, les rapports ou la journalisation avec d'autres infrastructures de sécurité dans l'organisation. Au fil du temps, cela peut augmenter la complexité, car les organisations utilisent souvent de multiples produits de sécurité ponctuels qui rendent leurs opérations moins efficaces dans ce domaine.

À l'heure où les entreprises cherchent des moyens d'améliorer l'expérience de leurs employés lorsqu'ils accèdent à Internet et aux applications web, les fonctionnalités cloud de la SWG du ZTNA 2.0 offrent une solution efficace qui supprime la latence et améliore la posture de sécurité globale (voir la figure 4-4).

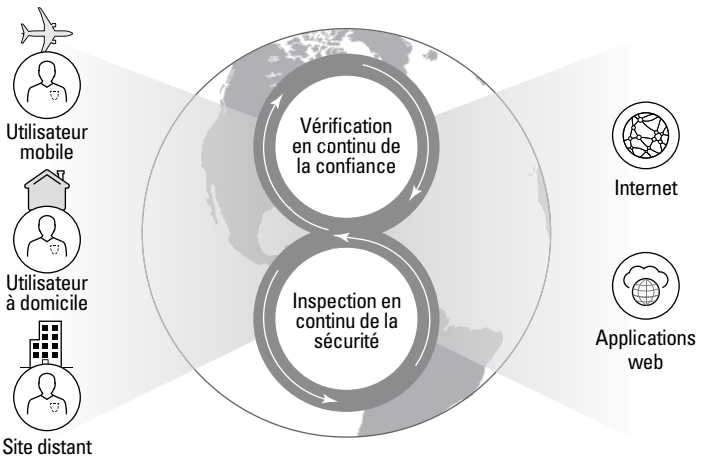

FIGURE 4-4 : Le ZTNA 2.0 en remplacement de la SWG/SWG cloud.

CONSEIL

Voici quelques exigences clés à prendre en compte lors de l'évaluation du ZTNA 2.0 pour remplacer des produits SWG existants :

- **Il ne nécessite pas de modifications importantes du réseau :** les organisations veulent pouvoir maintenir simplement les approches existantes basées sur des proxys afin de minimiser les perturbations et les remaniements majeurs du réseau.
- **Il offre une approche optionnelle basée sur des agents :** il est souhaitable d'avoir la possibilité d'installer un agent sur les terminaux des utilisateurs, mais cela ne doit pas être le seul modèle de déploiement disponible.
- **Il permet une application homogène des stratégies :** la solution doit permettre une mise en application cohérente des stratégies sur des effectifs hybrides comprenant des utilisateurs mobiles, à domicile et dans les sites distants.

SÉCURISATION DE L'ACCÈS À INTERNET POUR UNE ENTREPRISE PHARMACEUTIQUE FIGURANT AU CLASSEMENT FORTUNE 100

Une entreprise pharmaceutique du classement Fortune 100 souhaitait réduire ses déploiements sur site de matériel de divers fabricants et moderniser son infrastructure grâce à une sécurité en mode cloud.

Avec la migration croissante vers le cloud d'outils et d'applications dont les employés ont besoin pour faire leur travail, les solutions existantes ne pouvaient pas offrir une expérience transparente et répondre aux attentes, ce qui a entraîné une faible satisfaction globale des utilisateurs à l'égard de ces solutions en place.

Ce client avait besoin d'une approche moderne de la sécurité dans le cloud et a choisi la solution ZTNA 2.0 de Palo Alto Networks. Il a pu facilement migrer ses 100 000 utilisateurs en trois mois sans créer une nouvelle architecture réseau, le tout grâce aux capacités de proxy évidentes du ZTNA 2.0.

Sa nouvelle solution cloud-native a consolidé et éliminé son matériel de proxy sur site et lui a permis d'améliorer la sécurité pour tous les utilisateurs et tous les sites. Il a également déployé les fonctionnalités de Gestion autonome de l'expérience numérique (ADEM) de Prisma Access pour garantir des expériences utilisateur hors pair à tous les travailleurs hybrides.

Objectifs du projet

- Migrer vers le cloud
- Réduire le matériel sur site
- Améliorer l'expérience utilisateur

Impact

- 100 000 utilisateurs migrés en moins de trois mois
- Remplacement du matériel SWG sur site par une solution cloud-native
- Amélioration radicale de la posture de sécurité
- Expérience hors pair des utilisateurs grâce à l'ADEM

Sécurité avancée du SaaS

Il y a quelques années, les entreprises conservaient généralement toutes leurs applications et leurs données dans un data center sur site. Dans cet environnement, elles disposaient d'une visibilité totale et d'un contrôle granulaire sur les personnes qui accédaient à leurs applications et à leurs données et à quel moment, ainsi que sur les appareils (généralement des ordinateurs de bureau ou portables) utilisés pour y accéder.

Au fil du temps, lorsque les entreprises ont transféré leurs données dans le cloud et commencé à utiliser des services cloud tels que les applications SaaS, elles ont découvert qu'elles ne savaient plus qui accédait à leurs applications et données stockées dans le cloud et qui les utilisait, pas plus que – grâce à l'avènement des technologies mobiles comme les ordinateurs portables et les smartphones – les appareils utilisés pour accéder à ces services. En outre, l'omniprésence et la facilité d'adoption des applications SaaS conduisent souvent à un « shadow IT », dans le cadre duquel les utilisateurs utilisent des applications non autorisées ou non approuvées à des fins professionnelles, ce qui expose par inadvertance les données sensibles à un risque accru.

En raison de ce manque de visibilité, il est difficile pour les entreprises de protéger leurs données et elles s'exposent à une multitude de risques liés à la sécurité, tels que les violations de données, la non-conformité aux réglementations, les malwares, les ransomwares, etc.

Pour relever ces défis, les fournisseurs de solutions de sécurité ont mis au point des solutions CASB (Cloud Access Security Broker). Les CASB aident les entreprises à savoir où se trouvent leurs données dans les applications SaaS, et quand elles sont en mouvement dans les environnements de services cloud, les data centers sur site et parmi les travailleurs mobiles. Un CASB applique également les stratégies de sécurité, de gouvernance et de conformité d'une organisation, permettant aux utilisateurs autorisés d'accéder aux applications cloud et de les utiliser, tout en permettant aux organisations de protéger leurs données sensibles de manière efficace et homogène sur de multiples sites.

Toutefois, les solutions CASB classiques ne sont pas en mesure d'intégrer rapidement de nouvelles applications cloud, car elles reposent sur des bibliothèques d'applications statiques qui sont alimentées manuellement. Les applications de collaboration modernes telles que Slack, Zoom, Confluence et Jira, auxquelles les utilisateurs consacrent la majeure partie de leur temps de nos jours, ne sont généralement pas couvertes par les protections de l'interface de programmation d'application (API) offertes par ces solutions CASB.

Une solution CASB classique offre des capacités de sécurité cloud de base, limitées en termes d'étendue et de profondeur, et ne fournit qu'une sécurité fragmentaire. Par exemple, ses capacités en matière de prévention des pertes de données (DLP) sont assez basiques et imprécises, ne couvrant que les données de certaines applications SaaS tout en étant complètement détachées de toute solution DLP protégeant le reste de l'entreprise. Elles ne disposent pas non plus des mécanismes essentiels de protection contre les menaces qui permettent de détecter les variations infinies des menaces que les cybercriminels utilisent constamment pour cibler les applications SaaS.

JARGON TECHNIQUE

Lorsque les solutions CASB ont été développées pour la première fois, elles ont été conçues comme une solution ponctuelle et autonome, basée sur un proxy. Le problème des CASB basés sur un proxy est qu'ils nécessitent une redirection complexe du trafic à partir du pare-feu réseau, avec des agents d'autoconfiguration du proxy (PAC) et des collecteurs de journaux, ce qui entraîne une complexité architecturale et opérationnelle importante ainsi qu'un coût de possession élevé.

Les entreprises qui utilisent des solutions CASB traditionnelles ne peuvent pas suivre le rythme de croissance rapide des applications SaaS et du Shadow IT, la croissance omniprésente des données ou le nombre croissant de travailleurs hybrides et distants. Le remplacement de l'ancienne solution CASB par des capacités CASB de

nouvelle génération, fournies dans une architecture de périmètre de service d'accès sécurisé (SASE) qui englobe le ZTNA 2.0, permet aux entreprises d'adopter en toute sécurité des services cloud avec une vérification de la confiance et une inspection de la sécurité en continu, et des capacités qui incluent les éléments suivants (voir la figure 4-5) :

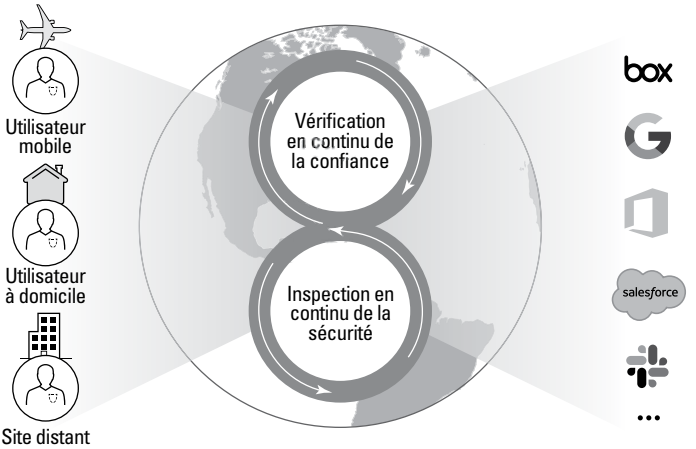

FIGURE 4-5 : Le ZTNA 2.0 pour une sécurité avancée des applications SaaS et une solution CASB de nouvelle génération.

- Visibilité et contrôle des applications SaaS
- Protection des applications SaaS approuvées
- Solution DLP avancée

SÉCURITÉ AVANCÉE DES APPLICATIONS SaaS POUR UN GRAND FOURNISSEUR AUTOMOBILE

Un leader mondial de la technologie automobile, qui emploie plus de 190 000 personnes dans des centaines de sites de production, dispose de dizaines de centres techniques importants dans le monde entier et est présent dans plus de 40 pays, comptait sur un grand nombre d'applications dans le cloud. Il avait besoin d'une meilleure

(suite)

(suite)

visibilité et d'un contrôle granulaire sur les applications SaaS connues et inconnues, d'une gestion consolidée des produits multifournisseurs et d'une inspection en ligne des menaces.

L'entreprise souhaitait pouvoir également créer et déployer simplement des politiques sans avoir recours à un proxy ou à des agents. Elle voulait en outre éliminer la nécessité de synchroniser les risques, les stratégies et les objectifs sur une couche distincte de la pile.

La solution ZTNA 2.0 de Palo Alto Networks, dotée de fonctionnalités CASB de nouvelle génération, a permis à l'entreprise de ne plus avoir à mettre à jour et à configurer les agents pour l'inspection en ligne, et de protéger les terminaux non gérés.

Objectifs du projet

- Adoption massive du cloud/SaaS
- Visibilité et contrôle des applications connues et inconnues
- Réduction de la complexité, consolidation de la sécurité

Impact

- Simplification du déploiement et de la création de stratégies en matière de sécurité dans le cloud
- Amélioration spectaculaire de la visibilité et du contrôle de toutes les applications
- Protection homogène pour 190 000 utilisateurs dans le monde entier

DANS CE CHAPITRE

- Assurer une visibilité et un contrôle complets
- Assurer une vérification en continu de la confiance
- Sécuriser toutes les applications dans une solution unifiée
- Appliquer une inspection de sécurité complète
- Prévenir la perte des données dans tous les environnements
- Garantir la disponibilité et les performances des applications
- Réduire la complexité et les coûts grâce à une seule solution

Chapitre 5
Dix questions (ou presque) à poser à votre fournisseur ZTNA 2.0

Voici quelques questions importantes pour vous aider à évaluer les fournisseurs potentiels d'accès réseau Zero Trust (ZTNA) 2.0 et leurs solutions.

Fournissez-vous une visibilité complète des applications de la couche 7 ?

Les utilisateurs ont de plus en plus recours à des applications diverses – dont une multitude d'applications SaaS (logiciel en tant que service) à partir d'une multitude d'appareils et de lieux – pour faire leur travail et pour leurs démarches personnelles. Beaucoup d'applications, comme la messagerie instantanée (IM) le partage de fichiers peer-to-peer (P2P) et le protocole Voix sur IP (VoIP), peuvent s'exécuter sur des ports et des adresses IP non standard ou dynamiques.

De plus, les utilisateurs en savent assez pour forcer des applications à s'exécuter sur des ports non standard à l'aide de protocoles de type RDP (Remote Desktop Protocol) ou SSH (Secure Shell), quelle que soit la politique de l'organisation à l'égard d'applications variées (approuvées, tolérées ou non approuvées). Ainsi, une solution ZTNA qui identifie les applications sur la base d'affectations arbitraires de ports de la couche 3 et qui se limite au contrôle d'accès de la couche 3 ou 4 n'est plus suffisante pour protéger votre entreprise.

CONSEIL

Recherchez une solution ZTNA 2.0 capable, par défaut, de classer le trafic par application sur tous les ports ; et qui ne crée pas de fardeau administratif en vous demandant de rechercher quelles applications utilisent quels ports pour pouvoir configurer les stratégies et règles appropriées. Une solution ZTNA 2.0 complète offre une entière visibilité de la couche 7 (application) sur l'utilisation des applications, et intègre des fonctionnalités permettant de comprendre et de contrôler leur utilisation.

Fournissez-vous une vérification en continu de la confiance ?

Le principe fondamental du Zero Trust est de « ne jamais faire confiance, toujours vérifier », et non de « ne jamais faire confiance, vérifier une fois » ou de « ne jamais faire confiance, vérifier occasionnellement ». Faire confiance à une entité sur la base d'identifiants de compte statiques vérifiés une fois sur un appareil qui semble légitime à un moment donné est synonyme de désastre. Les cybercriminels exploitent ce modèle de confiance imparfait pour se déplacer librement dans un environnement réseau après avoir franchi les défenses du périmètre.

CONSEIL

Une solution ZTNA 2.0 robuste fournit une vérification en continu de la confiance basée sur le comportement individuel de l'utilisateur, en tirant parti du machine learning (ML) pour déterminer le risque et identifier les menaces potentielles. L'accès au réseau ou à une application ne doit être autorisé qu'après un contrôle minutieux des utilisateurs et des appareils, notamment à l'aide de l'authentification multifacteur (MFA). Et ce n'est pas tout. La vérification de la confiance doit se faire de manière continue et transparente tout au long de la session afin de s'assurer que la posture de sécurité de l'utilisateur ou de l'appareil n'a pas changé ou n'a pas été compromise.

Sécurisez-vous de manière homogène toutes les applications par le biais d'un même produit ?

Comme nous l'avons vu au chapitre 1, les solutions de sécurité ponctuelles qui ne protègent que des applications spécifiques ou ne prennent en charge que des scénarios d'utilisation limités sont source de complexité, d'inefficacité et, en fin de compte, d'affaiblissement de la posture de sécurité. Les utilisateurs trouveront de nouveaux moyens créatifs de contourner les contrôles de sécurité qui sont déroutants et peu pratiques à utiliser. Les équipes de sécurité sont plus susceptibles de commettre des erreurs lors de la configuration et de l'utilisation d'outils ayant des systèmes d'exploitation, des interfaces et des syntaxes différents. Elles seront en outre submergées par des alertes qui ne peuvent pas être facilement corrélées à des menaces spécifiques dans une solution intégrée.

CONSEIL

Votre solution ZTNA 2.0 doit sécuriser de manière homogène toutes vos applications, qu'il s'agisse d'applications personnalisées existantes, d'applications modernes basées sur des microservices, d'applications SaaS ou autres, dans un seul et même produit unifié.

Appliquez-vous une inspection de sécurité complète ?

Une solution ZTNA 2.0 ne doit pas se contenter d'autoriser ou de bloquer le trafic sur la base d'une inspection limitée des en-têtes des paquets et de l'application de règles de pare-feu statiques. Elle doit également prévenir les malwares avancés, y compris les ransomwares, et rechercher les menaces connues et inconnues dans le trafic des applications et des données (chiffrées ou non) et ce, pour l'ensemble du trafic des applications, et pas seulement le trafic des applications privées.

CONSEIL

Une solution ZTNA 2.0 complète doit fournir une inspection et un contrôle complets de la sécurité, y compris la prévention des malwares et des menaces.

Protégez-vous de manière homogène toutes les données de l'entreprise ?

Pour que la protection des données soit systématique, il faut consolider les stratégies de protection des données dans tous les environnements et tous les vecteurs de communication de données. Si les stratégies et configurations de protection des données sont déconnectées pour différentes applications SaaS, des référentiels sur site, des communications

par courrier électronique, ou encore un stockage local, cela entraîne des angles morts en matière de sécurité, une complexité de gestion, des contrôles irréguliers et le Shadow IT.


CONSEIL

Choisissez une solution ZTNA 2.0 qui permet une stratégie homogène de prévention des pertes de données (DLP) dans tous les environnements où les données vivent et circulent, quel que soit leur emplacement.

Fournissez-vous des accords de niveau de service sur le temps de fonctionnement et les performances pour toutes les applications ?

Les outils de sécurité qui ont un impact négatif sur le temps de fonctionnement et les performances des applications contribueront à une mauvaise expérience pour l'utilisateur, ce qui finit par entraîner une augmentation du Shadow IT, les utilisateurs cherchant de nouveaux moyens de contourner les outils censés les protéger.


CONSEIL

Les solutions modernes ZTNA 2.0 sont fournies via le cloud et offrent donc des garanties de fiabilité et de performance qui permettent aux utilisateurs de votre organisation d'utiliser les applications dont ils ont besoin – y compris les applications internes et les applications SaaS – de manière sécurisée et efficace, quand ils en ont besoin. Assurez-vous que votre fournisseur ZTNA 2.0 propose des accords de niveau de service (SLA) sur la disponibilité et les performances qui répondent aux besoins de votre organisation.

Disposez-vous d'un seul produit unifié pour sécuriser l'entreprise ?

Les outils de sécurité cloisonnés qui ne peuvent pas être facilement intégrés à d'autres solutions augmentent le coût et la complexité de votre environnement et peuvent retarder la détection des menaces critiques, leur mise en corrélation, leur identification et la réponse à apporter. Ce surcroît de complexité entraîne en fin de compte une augmentation des frais généraux de gestion tout en augmentant considérablement les risques et l'exposition.


CONSEIL

Un fournisseur ZTNA 2.0 doit offrir une seule solution unifiée, comme un périmètre de service d'accès sécurisé (SASE), qui protège l'ensemble de votre entreprise – y compris les utilisateurs, les applications, les appareils et les données –, quel que soit l'emplacement, afin de réduire les risques et d'obtenir de meilleurs résultats en matière de sécurité.

Glossaire

accès réseau Zero Trust (ZTNA) : attitude de sécurité qui vise à « ne jamais faire confiance, toujours vérifier » pour garantir aux utilisateurs un contexte approprié par le biais de l'authentification et de la vérification des attributs avant d'autoriser l'accès à des applications ou données dans le cloud ou le data center.

accord de niveau de service (SLA) : normes officielles de performances minimales pour les systèmes, applications, réseaux ou services.

ADEM : *voir* Gestion autonome de l'expérience numérique (ADEM).

analyse du comportement des utilisateurs et des entités (UEBA) : solution ou fonctionnalité de cybersécurité qui détecte les menaces en identifiant une activité qui s'écarte d'une référence normale. Bien que l'UEBA puisse être utilisée pour diverses raisons, elle sert généralement à surveiller et à détecter des schémas de trafic inhabituels, des accès et des mouvements de données non autorisés ou des activités suspectes ou malveillantes sur un réseau informatique ou des terminaux.

analyse du trafic réseau (NTA) : catégorie d'outils servant à intercepter, à enregistrer et à analyser les modèles de trafic réseau pour détecter et répondre aux anomalies et aux activités suspectes grâce à une combinaison de fonctionnalités de machine learning, de modélisation comportementale et de détection basée sur des règles. *Voir aussi* machine learning.

Antivirus (AV) : logiciel conçu pour détecter et empêcher les virus informatiques et autres malwares d'infecter un système. *Voir aussi* Malware.

API (Application Programming Interface) : *voir* interface de programmation d'application (API).

authentification multifacteur (MFA) : mécanisme d'authentification nécessitant deux ou plusieurs des facteurs suivants : ce que vous savez, ce que vous possédez et ce que vous êtes. Par exemple, un utilisateur peut s'authentifier à l'aide de son nom d'utilisateur et de son mot de passe (ce qu'il sait) et d'un code d'accès à usage unique envoyé sur un téléphone mobile préalablement enregistré auprès de l'organisation (ce qu'il possède).

Autonomous Digital Experience Management (ADEM) : fonctionnalité de Palo Alto Networks Prisma Access qui fournit une surveillance de l'expérience numérique SASE-native et une visibilité complète pour résoudre les problèmes de connectivité des utilisateurs de manière autonome, avant ou lorsqu'ils surviennent. *Voir aussi* périmètre de service d'accès sécurisé (SASE).

AV : *voir* antivirus (AV).

C2 : *voir* commande et contrôle (C2).

centre opérationnel de sécurité (SOC) : site de cybersécurité qui assure la surveillance, l'évaluation, la défense et la résolution des incidents sur les ressources informatiques et réseau des entreprises, y compris les environnements sur site et cloud

cloud hybride : environnement composé de ressources provenant de plusieurs clouds publics et/ou privés qui assurent la portabilité des applications et des données entre les clouds. *Voir aussi* cloud privé *et* cloud public.

cloud privé : modèle de déploiement de cloud computing composé d'une infrastructure cloud utilisée par une seule organisation.

cloud public : modèle de déploiement de cloud computing composé d'une infrastructure cloud ouverte au public.

commande et contrôle (C2) : trafic de communications entre des malwares et/ou des systèmes compromis et l'infrastructure du serveur à distance d'un attaquant qui sert à envoyer et recevoir des commandes malveillantes ou à exfiltrer des données.

détection et réponse sur les terminaux (EDR) : catégorie d'outils servant à détecter et à examiner les menaces sur les terminaux. Les outils EDR intègrent généralement des fonctionnalités de détection, d'investigation, de réponse et de traque des menaces (threat hunting).

DLP : *voir* prévention des pertes de données (DLP).

DNS (Domain Name System) : *voir* système de noms de domaine (DNS).

DPI : *voir* inspection approfondie des paquets (DPI) :

EDR : *voir* détection et réponse sur les terminaux (EDR).

EPP : *voir* plateforme de protection des terminaux (EPP).

exploit : logiciel ou code qui exploite une vulnérabilité dans un système d'exploitation ou une application et y provoque un comportement inattendu. Par exemple, une escalade de privilèges, un contrôle à distance ou une attaque par déni de service.

fichier d'autoconfiguration du proxy (PAC) : ensemble de règles JavaScript qui indiquent à un terminal comment diriger son trafic pour une URL donnée : via un proxy web ou directement vers Internet. Il peut contenir des informations telles que l'adresse IP du site web, l'adresse IP de l'utilisateur et l'hôte qui a demandé le site web. *Voir aussi* Uniform Resource Locator (URL).

FWaaS : *voir* pare-feu en tant que service (FWaaS).

gestion des informations et des événements de sécurité (SIEM) : système permettant de collecter, d'analyser, de corréler et de présenter des journaux et des alertes de sécurité en temps réel. Les analystes des centres opérationnels de sécurité (SOC) utilisent les outils SIEM pour gérer les incidents de sécurité, ainsi que pour détecter et répondre rapidement aux menaces potentielles. *Voir aussi* centre opérationnel de sécurité (SOC).

IA : *voir* Intelligence artificielle (IA).

inspection approfondie des paquets (DPI) : méthode avancée d'analyse et de gestion du trafic réseau allant au-delà des en-têtes initiaux des paquets.

intelligence artificielle (IA) : capacité d'un ordinateur à interagir avec son environnement, à en tirer des enseignements et à effectuer automatiquement des actions sans être explicitement programmé.

interface de programmation d'application (API) : ensemble de protocoles, de routines et d'outils servant à développer et à intégrer des applications.

IP : *voir* protocole Internet (IP).

IPS : *voir* système de prévention des intrusions (IPS).

LAN : *voir* réseau local (LAN).

logiciel en tant que service (SaaS) : modèle de distribution de logiciels en mode cloud dans lequel un fournisseur tiers héberge des applications qu'il met à la disposition des clients sur Internet. Le fournisseur héberge et gère les serveurs, les bases de données et le code qui constituent les applications.

machine learning (ML) : méthode d'analyse des données qui permet aux ordinateurs d'examiner un jeu de données et d'effectuer automatiquement des actions basées sur les résultats sans être explicitement programmés.

malware : logiciel ou code malveillant généralement conçu pour endommager ou désactiver un système informatique, en prendre le contrôle ou voler des informations qu'il renferme.

messagerie instantanée (MI) : type de chat en temps réel sur Internet.

MFA : *voir* authentification multifacteur (MFA).

MI : *voir* messagerie instantanée (MI).

ML : *voir* machine learning (ML).

modèle Open Systems Interconnection (OSI) : modèle de référence des réseaux composé de sept couches : physique, liaison, réseau, transport, session, présentation et application.

modèle OSI : *voir* modèle Open Systems Interconnection (OSI).

MPLS : *voir* Multiprotocol Label Switching (MPLS).

multicloud : environnement composé de ressources provenant de plusieurs clouds publics et/ou privés, mais qui ne fournit pas nécessairement la portabilité des applications et des données entre les clouds (autrement dit, les différents environnements cloud peuvent fonctionner de manière cloisonnée). À noter que si tous les environnements cloud hybrides sont également des environnements multicloud, tous les environnements multicloud ne sont pas nécessairement des environnements cloud hybrides. *Voir aussi* cloud hybride, cloud privé *et* cloud public.

Multiprotocol Label Switching (MPLS) : méthode de transmission de paquets à travers un réseau qui utilise des étiquettes insérées entre les en-têtes des couches 2 et 3 du paquet.

NTA : *voir* analyse du trafic réseau (NTA).

P2P : *voir* peer-to-peer (P2P).

PAC : *voir* fichier d'autoconfiguration du proxy (PAC).

pare-feu en tant que service (FWaaS) : pare-feu proposé sous forme de service dans un environnement cloud.

passerelle web sécurisée (SWG) : plateforme ou service de sécurité dont l'objectif est de maintenir une visibilité sur tous les types de trafic, tout en bloquant les contournements symptomatiques d'une éventuelle menace. Une passerelle web sécurisée peut également intégrer des fonctionnalités de filtrage des contenus web et de prévention des vols d'identifiants.

peer-to-peer (P2P) : architecture d'applications distribuées qui permet le partage entre nœuds.

périmètre défini par logiciel (SDP) : un périmètre défini par logiciel sécurise toutes les connexions aux services fonctionnant sur une infrastructure réseau, sur toutes les couches, en fonction du niveau de sécurité défini.

plateforme de protection des terminaux (EPP) : suite intégrée de technologies de sécurité des terminaux (antivirus, chiffrement des données, prévention des pertes de données, pare-feu personnel, contrôle des ports et des appareils, etc.).

prévention des pertes de données (DLP) : application ou appareil permettant de détecter le stockage ou la transmission non autorisé(e) de données sensibles.

protocole Internet (IP) : protocole de la couche 3 du modèle OSI sur lequel se base l'Internet moderne. *Voir aussi* modèle Open Systems Interconnection (OSI).

RDP : *voir* Remote Desktop Protocol (RDP).

Remote Desktop Protocol (RDP) : protocole Microsoft propriétaire qui fournit un accès à distance à un ordinateur. Le protocole RDP utilise par défaut le port TCP 3389 et le port UDP 3389 *Voir aussi* Transmission Control Protocol (TCP) *et* User Datagram Protocol (UDP).

réseau étendu (WAN) : réseau informatique qui s'étend sur une zone géographique large et peut connecter plusieurs réseaux locaux. *Voir aussi* réseau local (LAN).

réseau étendu défini par logiciel (SD-WAN) : nouvelle approche du réseau étendu qui sépare le contrôle du réseau et les processus de gestion du matériel sous-jacent et les rend accessibles sous forme de logiciel. *Voir aussi* réseau étendu (WAN).

réseau local (LAN) : réseau informatique qui relie des ordinateurs dans une zone relativement petite, comme un immeuble de bureaux, un entrepôt ou une résidence.

réseau privé virtuel (VPN) : un VPN crée une connexion privée, appelée *tunnel*, avec Internet. Toutes les informations transmises à partir d'un appareil connecté à un VPN sont chiffrées et passent par ce tunnel. Lorsqu'il est connecté à un VPN, un appareil se comporte comme s'il se trouvait sur le même réseau local que le VPN. Le VPN transmet le trafic de l'appareil vers et depuis le site web ou le réseau concerné par le biais de sa connexion sécurisée.

SaaS : *voir* logiciel en tant que service (SaaS).

SDP : *voir* périmètre défini par logiciel (SDP).

SD-WAN : *voir* réseau étendu défini par logiciel (SD-WAN).

Secure Shell (SSH) : protocole de réseau cryptographique qui fournit un accès sécurisé à un ordinateur distant.

shadow IT : applications et services informatiques acquis et exploités par les utilisateurs sans autorisation explicite de leur organisation, et souvent sans l'approbation ou le support du service informatique.

SIEM : *voir* gestion des informations et des événements de sécurité (SIEM).

SLA : *voir* accord de niveau de service (SLA).

SOC : *voir* centre opérationnel de sécurité (SOC).

SSH : *voir* Secure Shell (SSH).

SWG : *voir* passerelle web sécurisée (SWG).

système de noms de domaine (DNS) : service de répertoire décentralisé et hiérarchique qui convertit les noms de domaine en adresses IP pour les ordinateurs, les services et d'autres ressources informatiques connectées à un réseau ou à Internet. *Voir aussi* protocole Internet (IP).

système de prévention des intrusions (IPS) : périphérique matériel ou application logicielle qui détecte et bloque les intrusions présumées au sein d'un réseau ou d'une machine hôte.

tactiques, techniques et procédures (TTP) : comportements, méthodes, stratégies et outils dont les cybercriminels se servent pour attaquer une cible.

TCP : *voir* Transmission Control Protocol (TCP).

Transmission Control Protocol (TCP) : protocole orienté connexion qui établit une connexion entre deux hôtes et garantit la livraison des données et des paquets dans le bon ordre.

tromboning : pratique consistant à acheminer le trafic réseau via un point de contrôle (par ex., un pare-feu).

TTP : *voir* tactiques, techniques et procédures (TTP).

UDP : *voir* User Datagram Protocol (UDP).

UEBA : *voir* analyse du comportement des utilisateurs et des entités (UEBA).

Uniform Resource Locator (URL) : couramment dénommée « adresse web ». Identificateur unique d'une ressource connectée à Internet.

URL : *voir* Uniform Resource Locator (URL).

User Datagram Protocol (UDP) : protocole réseau qui ne garantit pas la livraison des paquets ni leur ordre de livraison sur un réseau.

VoIP : *voir* voix sur IP (VoIP).

voix sur IP (VoIP) : protocoles de téléphonie conçus pour transporter des communications vocales sur des réseaux TCP/IP. *Voir aussi* Transmission Control Protocol (TCP) *et* protocole Internet (IP).

VPN : *voir* réseau privé virtuel (VPN).

WAN : *voir* réseau étendu (WAN).

Zero Trust : initiative stratégique qui permet de prévenir les compromissions en éliminant la notion de confiance implicite dans votre organisation. Fondé sur le principe de « ne jamais faire confiance, toujours vérifier », le Zero Trust est conçu pour empêcher tout mouvement latéral

ZTNA : *voir* accès réseau Zero Trust (ZTNA).

Zero Trust with Zero Exceptions

ZTNA 1.0 is over. Secure the future of hybrid work with ZTNA 2.0. Only available with Prisma® Access.

Palo Alto Networks Prisma® Access protects the hybrid workforce with the superior security of ZTNA 2.0 while providing exceptional user experiences from a simple, unified security product. Purpose-built in the cloud to secure at cloud scale, only Prisma Access protects all application traffic with best-in-class capabilities while securing both access and data to dramatically reduce the risk of a data breach.

Learn how Prisma Access secures today's hybrid workforce without compromising performance, backed by industry-leading SLAs to ensure exceptional user experiences.

https://www.paloaltonetworks.com/sase/ztna

Commencez à utiliser le ZTNA dès aujourd'hui

Les effectifs hybrides et les architectures à connectivité directe avec les applications ont rendu les solutions de sécurité traditionnelles obsolètes tout en élargissant la surface d'attaque de façon exponentielle. Dans le même temps, les menaces augmentent en fréquence et en sophistication tandis que la prolifération d'outils de sécurité disparates crée une complexité opérationnelle. Les solutions de sécurité cloud existantes offrent trop d'accès avec une protection insuffisante, fournissent une sécurité inégale et incomplète entre les applications et se traduisent par des performances et des expériences utilisateur médiocres. L'accès réseau Zero Trust 2.0 constitue une meilleure voie à suivre.

À l'intérieur…

- Découvrez des cas d'utilisation pour commencer votre parcours ZTNA 2.0
- Comprenez les différences entre le ZTNA 2.0 et les solutions ZTNA existantes
- Apprenez les cinq principes du ZTNA 2.0
- Identifiez les questions à poser à votre fournisseur ZTNA
- Découvrez comment une solution unifiée offre des expériences hors pair aux utilisateurs

paloalto® NETWORKS

Lawrence Miller a exercé en tant que Chief Petty Officer dans la marine américaine et travaille depuis plus de 25 ans dans les départements informatiques de divers secteurs. Il a co-écrit *CISSP For Dummies* et plus de 200 autres livres *pour les Nuls* portant sur diverses questions de sécurité et de technologie.

Allez sur Dummies.com®
pour voir des vidéos, des tutoriels en photos, des articles pratiques ou pour faire des achats !

ISBN: 978-1-394-18372-2

pour les nuls®

WILEY END USER LICENSE AGREEMENT

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