netskope

Livre blanc

Le rôle historique et à venir des Pare-feux et des Passerelles de proxy

TABLE DES MATIÈRES

INTRODUCTION

À qui s'adresse ce livre blanc ?

Vice-présidents, architectes, dirigeants et responsables réseau et sécurité.

Quand lire ce livre blanc ?

Lors de la planification des futurs points de contrôle en ligne pour la protection des données et contre les menaces.

Pourquoi le lire ?

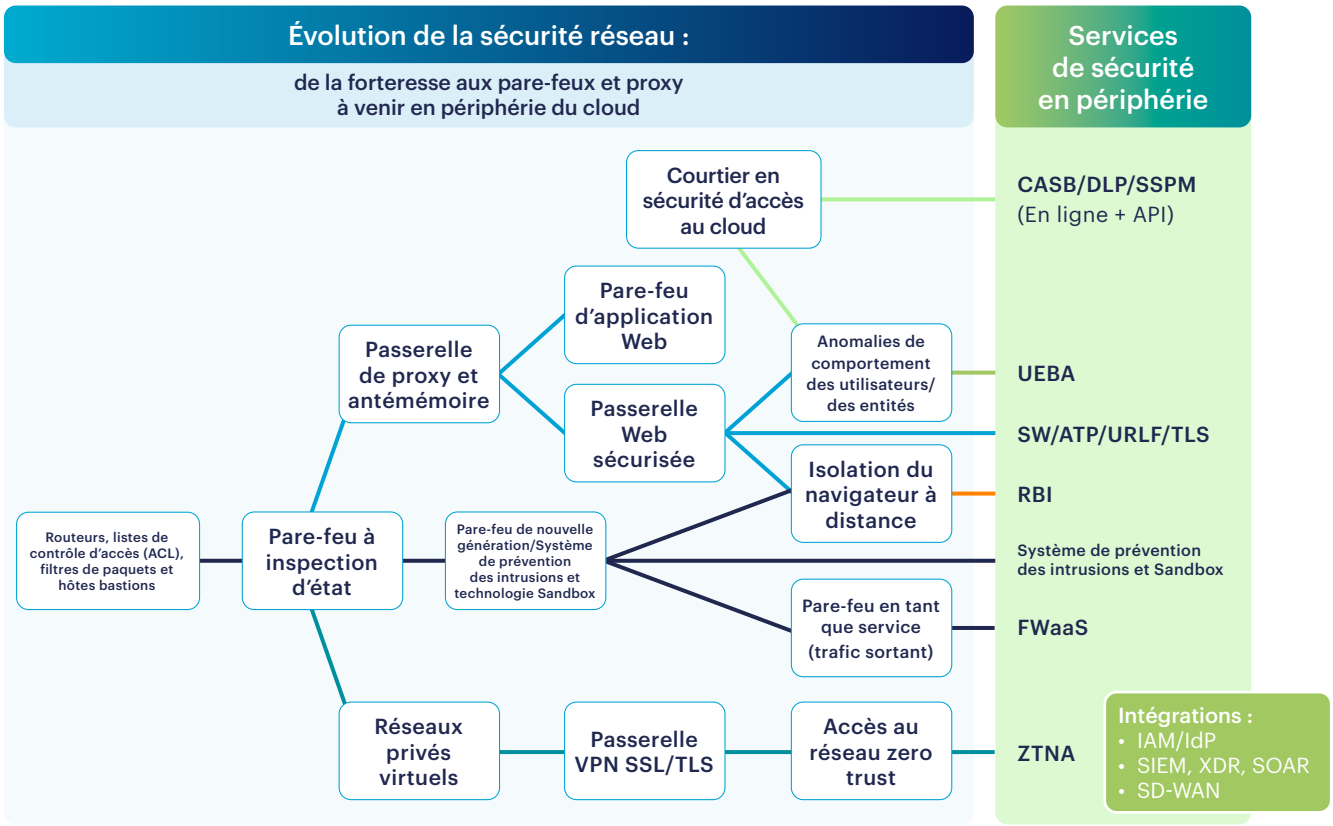
Le rôle des pare-feux et des passerelles de proxy évolue en fonction du contenu et du contexte pour un accès adaptatif, des principes du zero trust et un travail à distance et hybride reposant sur les services de sécurité en périphérie (SSE).

RÉSUMÉ

En général, les êtres humains n'apprécient pas le changement et la répétition d'une même tâche dans l'espoir d'obtenir de meilleurs résultats est une définition de la folie. Le changement générationnel inévitable du domaine des hautes technologies qui se produit tous les cinq à sept ans vient creuser l'écart entre la résistance humaine au changement et l'avancée de la technologie. Le débat ancien opposant les pare-feux aux passerelles de proxy est récemment entré dans une nouvelle génération. Pour les mettre en perspective, il est nécessaire de comprendre les divisions historiques des années passées et l'évolution plus récente de ces systèmes après la pandémie. Le rôle de l'accès à distance a également changé avec l'adoption croissante du travail hybride tandis que les principes du zero trust remettent en question des pratiques de sécurité suivies depuis longtemps. Il y a des années, les passerelles de proxy avaient des rôles bien distincts : les passerelles Web sécurisées (SWG) pour le trafic sortant et les pare-feux d'application Web (WAF) pour le trafic entrant. Nous constatons aujourd'hui une même séparation quant aux pare-feux de nouvelle génération (NGFW), le trafic sortant du travail hybride et du télétravail au sein des plateformes de services de sécurité en périphérie (SSE) relevant du firewall-as-a-service (FWaaS) hébergé dans le cloud tandis que les pare-feux contrôlant le trafic entrant/sortant restent en place pour protéger les datacenters, l'infrastructure et les employés sur site. L'accès réseau zero trust (ZTNA) remplace également les réseaux privés virtuels (VPN) présentant des services exploitables sur Internet et des problèmes connus de mouvement latéral par un modèle de connexion « à l'envers » plus sécurisé qui s'applique directement aux applications ou aux ressources souhaitées.

> L'IA et l'apprentissage automatique sont des moteurs évidents de ce changement générationnel et requièrent la connaissance du contenu et du contexte dont manquent la plupart des lignes de défense existantes pour l'analyse en temps réel.

L'élément crucial est l'impact sur la protection des données et contre les menaces en ligne, là où un modèle vieux de plusieurs décennies de signature par hachage de fichiers pour les fichiers malveillants ou les données sensibles n'est plus adapté, même avec un partage fréquent de renseignements sur les menaces parmi les utilisateurs pour les indicateurs de compromission (IOC). Les menaces inconnues et de type « zero-day » continuent de s'accroître et les environnements aux données dynamiques et non structurées (par exemple le code source) changent trop rapidement pour que celles-ci soient classées et enregistrées par le système de prévention des pertes de données. Dans ces cas d'utilisation qui se multiplient, le recours à l'IA et à l'apprentissage automatique comble cette lacune en temps réel tout en offrant une expérience utilisateur performante. Nous sommes dans une ère nouvelle, et pour l'architecture réseau et de sécurité, il est vital de comprendre le parcours suivi jusqu'ici et ce que ces nouveaux rôles signifient. Analyser le contenu et le contexte en temps réel et accepter les changements seront les clés de la réussite.



DÉBUTS ET DIVISION

Routeurs, listes de contrôle d'accès (ACL), filtres de paquets et hôtes bastions

Pour la plupart des gens, l'arrivée d'Internet s'est faite au milieu des années 90, via des modems à numérotation offrant des textes aux images statiques sans rien de commun avec ce que connaissons aujourd'hui. Les listes de contrôle d'accès (ACL) définissaient l'accès entrant et sortant sur des routeurs, tandis que dans un cercle restreint, des initiés partageaient leurs connaissances sur les nouvelles conceptions de pare-feux notamment les doubles hôtes bastions et le kit d'outils pour pare-feu (fwtk). Internet était une destination externe et certains prétendaient même qu'il s'agissait de la radio CB des années 90 et qu'il disparaîtrait. Une distinction entre le trafic entrant et sortant était établie depuis le début pour les ACL, les routeurs, les filtres de paquets et les conceptions de pare-feux initiales, qu'ils soient basés sur un proxy ou le réseau.

Les pare-feux à inspection d'état prévalent grâce à leurs performances

Une fois que le concept d'Internet a été adopté pour partager les informations en ligne, communiquer avec ses pairs et acquérir des connaissances, rien ne pouvait arrêter cette dynamique. La popularité d'Internet était telle que certaines personnalités politiques auraient même revendiqué sa création. La vitesse était un facteur essentiel et les performances des pare-feux de réseau à inspection d'état dépassaient de loin celles des conceptions de double hôte bastion et de proxy, avec des vitesses 8 à 10 fois supérieures. On ouvrait les ports de sortie pour les demandes approuvées selon des règles puis on les fermait une fois la session terminée, ou on les mémorisait pour le trafic entrant, ce qui améliorait les ACL statiques en maintenant les ports ouverts. Le trafic était défini pour des adresses IP source et cible spécifiques, des ports et des protocoles spécifiques, ce que l'on a qualifié de contrôle d'accès à 5 tuples. Le pare-feu est alors devenu la principale défense permettant aux équipes de sécurité de définir l'intérieur et l'extérieur, complétée par une DMZ destinée aux services hébergés tels que des serveurs Web et de partage de fichiers.

Réseaux privés virtuels et pare-feux de nouvelle génération

L'accès à distance est rapidement devenu un cas d'utilisation répandu et les réseaux privés virtuels (VPN) sont un élément essentiel des pare-feux basés sur le réseau pour évoluer finalement vers un accès à distance basé sur le navigateur via SSL. Les VPN permettaient aux employés d'accéder à distance à des zones spécifiques du réseau, et aux sous-traitants, partenaires et tiers dont les applications et données internes leur étaient accessibles avec un mouvement latéral d'une certaine latitude. Les sites Web continuaient d'étendre leurs fonctionnalités, le filtrage du Web et les catégories d'URL prenaient de la maturité et l'on distinguait le bon côté d'Internet de ses mauvais aspects. Les sites Web et domaines populaires ont commencé à ressembler aux applications et le pare-feu de nouvelle génération (NGFW) est apparu, offrant des contrôles d'accès basés sur les ID des applications, des contenus et des utilisateurs, un premier pas vers les contrôles d'accès à 5 tuples.

Le proxy se divise en deux catégories : les passerelles Web sécurisées et les pare-feux d'application Web

L'inspection par proxy a connu un certain succès, tandis que ses adeptes ont fait valoir sa conception plus sécurisée, basée notamment sur la reconstruction du contenu pour l'analyse de sécurité au lieu d'un antivirus appliqué au flux par les NGFW. L'inspection par proxy offrait également la conformité des protocoles, des contrôles basés sur les en-têtes et des règles granulaires donnant la possibilité de filtrer, retirer ou remplacer des objets Web. Toutefois, en raison de leurs problèmes de performances, les proxys étaient moins adoptés que l'inspection d'état et les NGFW puissants aux règles de contrôle plus souples. La mise en antémémoire était devenue un cas d'utilisation clé des proxys pour les contenus souvent consultés, réduisant le parcours vers les serveurs d'origine des contenus et améliorant l'expérience utilisateur. À l'apogée de la mise en antémémoire, les utilisateurs pouvaient accélérer de plus de 30 % le contenu Web, mais ce pourcentage a diminué à mesure que les sites Web devenaient plus dynamiques et personnalisés. Le réel bénéfice de la mise en antémémoire était une nouvelle conception des serveurs proxy créés sur des systèmes d'exploitation optimisés conçus pour les objets Web plutôt que pour des fichiers et des exécutables, ainsi que des performances plus rapides.

> Les fonctions d'entrée et de sortie des serveurs proxys étaient séparées, la sortie étant définie par les passerelles Web sécurisées (SWG) et l'entrée par les pare-feux d'application Web (WAF). Cependant, cette même division s'appliquera aux NGFW plusieurs décennies plus tard dans le sillage de la pandémie.

AVANT LA DOMINATION DU PROTOCOLE TLS, LES DÉBUTS DE L'ÉVOLUTIVITÉ DU MATÉRIEL

Inspection HTTP du texte en clair

Les NGFW ont continué leur montée en puissance, ainsi que les passerelles de proxy (ou les SWG), car ils présentaient l'avantage d'une inspection HTTP du texte en clair et de ne nécessiter le chiffrement SSL, puis TLS, que d'un petit pourcentage du trafic. Avant que cet angle mort ne se développe, les NGFW, les systèmes de protection contre les intrusions (IPS) et les SWG pouvaient inspecter facilement des contenus de texte en clair à des fins de filtrage du Web, de contrôle de fichiers par anti-virus et de contrôle d'accès. Un problème important est survenu quand des utilisateurs internes malveillants ont trouvé l'astuce d'exploiter les commandes release et renew pour obtenir une nouvelle affectation temporaire d'adresse IP et ainsi masquer leur identité. Les équipes des ressources humaines ne pouvaient pas avoir la certitude d'avoir le bon employé en cas de violation de règles, et encore moins quand il était recherché par les autorités locales ou fédérales. Cela a accru l'intérêt porté aux SWG qui offraient une authentification et une autorisation intégrées en fonction de la session, car l'identité de l'utilisateur était passible de sanction quel que soit le nombre de modifications de l'affectation temporaire de l'adresse IP. Un deuxième problème majeur était l'évolution des menaces, pour lesquelles il est devenu souhaitable de suspendre et ralentir le téléchargement des fichiers afin de donner plus de temps de détection aux systèmes de défense contre les logiciels malveillants. Aujourd'hui, nous appelons cela la protection par recherche du patient zéro.

Émergence du trafic chiffré

> Le chiffrement du trafic par SSL puis TLS est devenu plus populaire et a créé un angle mort pour les défenses de sécurité réseau.

L'activation de l'inspection SSL/TLS du trafic pouvait surcharger l'appliance NGFW utilisée pour l'inspection du trafic HTTP en clair, c'est pourquoi cette solution était souvent évitée. Pour l'inspection SSL/TLS, on a recouru de plus en plus à des SWG dédiées qui présentaient en outre l'avantage de filtrer, retirer ou remplacer n'importe quel objet Web et de ralentir les fichiers pour donner plus de temps aux défenses contre les logiciels malveillants. Le filtrage statique des URL a également évolué vers une notation dynamique des URL par l'apprentissage automatique qui permettait de déceler en temps réel les sites dignes de confiance. Avec en outre le petit avantage lié à la mise en antémémoire des contenus et aux dispositifs de séparation de flux, les SWG sont devenues le point de sortie du trafic Web principalement sur les ports 80 et 443 tandis que le NGFW maintenait la protection sur l'ensemble des ports et des protocoles et offrait de plus un accès à distance au VPN. À cette époque, le chiffrement du trafic SSL/TLS a augmenté de 15 % à 75 % en quelques années, et même les SWG peu sollicitées croulaient sous la surcharge du trafic chiffré. C'est ainsi que sont apparus les cartes accélératrices SSL et les dispositifs de déchargement SSL utilisés en couche dans une pile de défense pour une protection évoluée contre les menaces.

Différences entre les solutions entreprise et milieu de gamme

En matière de sécurité réseau en ligne, une caractéristique unique qui différencie les solutions pour grandes entreprises des solutions milieu de gamme est la capacité de gérer la solution par l'établissement de scripts. Les grandes entreprises préfèrent investir dans les langages de programmation et de script pour gérer les solutions de sécurité et ne sont pas très intéressées par une interface utilisateur d'administration Web. L'inverse est vrai pour les solutions de milieu de gamme, dans lesquelles une interface utilisateur d'administration Web propose un processus de règles à suivre pas à pas et convivial qui sert de guide. Aujourd'hui, ces solutions disposent de fonctionnalités de base telles qu'une couche d'interface de programmation sur laquelle on superpose une couche d'interface utilisateur pour répliquer ces fonctionnalités. Toutes les tâches que l'interface utilisateur peut accomplir traversent la couche d'interface de programmation et peuvent donc être écrites sous forme de script. Les groupes et les communautés d'utilisateurs, ainsi que les experts des différentes disciplines se partagent souvent des scripts plutôt que de regarder une démo d'interface utilisateur avec des instructions pas à pas, selon un indicateur clé des administrateurs d'entreprise.

LES RÔLES AVANT LA PANDÉMIE

Une décennie de SWG et de NGFW aux fonctions bien définies

Pendant bien plus d'une décennie, les fonctions des passerelles Web sécurisées et des pare-feux de nouvelle génération sont restées stables, et presque toutes les organisations présentes sur Internet avaient déployé un NGFW. Toutefois, les passerelles Web sécurisées n'étaient abordables que pour les organisations riches en ressources. Un facteur de changement au lent développement a été le trafic chiffré par SSL/TLS qui a placé un fardeau sur les appliances matérielles des pare-feux pour déchiffrer le trafic. Les NGFW ont continué d'inspecter les en-têtes de paquets, de filtrer les domaines et d'analyser le contenu visible tandis que les SWG devenaient spécialement adaptées à l'inspection du trafic chiffré, à l'analyse de contenu, à l'identification plus stricte des utilisateurs et offraient en outre la possibilité de filtrer, retirer ou remplacer des objets Web.

Les administrateurs connaissant les passerelles proxy Web étaient également très demandés à une époque où les effectifs et les budgets consacrés à la sécurité informatique étaient limités.

En matière d'enregistrement des événements, les NGFW se sont principalement concentrés sur les alertes tandis que les SWG enregistraient des événements détaillés sur les transactions Web en générant de forts volumes submergeant souvent les solutions de génération de rapports. Une SWG d'abord déployée pour l'inspection du trafic chiffré s'exécutait à moins de 10 % de sa capacité et à la fin de sa durée de vie de cinq ans, jusqu'à 75 % de sa capacité d'utilisation puis était prête à être remplacée, dans le meilleur des cas. Cependant, tous les déploiements ne pouvaient pas soutenir la forte croissance du trafic chiffré et l'adoption du cloud par Office 365 est venue contrarier les clients et créer des problèmes de budget.

Il en a résulté une utilisation généralisée des NGFW pour définir les périmètres et une utilisation plus limitée des SWG pour les organisations bénéficiant des ressources nécessaires pour déchiffrer et inspecter le trafic Web en vue d'une analyse en temps réel du contenu.

De nouvelles défenses face à l'inconnu

La méthode de sécurité traditionnelle consistant à appliquer des correctifs aux systèmes et à mettre à jour les signatures a été remise en question par de nouvelles URL, de nouveaux contenus et des menaces zero-day jamais vues auparavant. On disposait de deux options face à ce contenu inconnu et non évalué : l'analyser en ligne en faisant attendre l'utilisateur, ou l'envoyer aux défenses en arrière-plan à des fins d'analyse puis mettre à jour les signatures. Les SWG offraient l'avantage d'une inspection du trafic chiffré assurant la visibilité du contenu qui permettait d'évaluer et de catégoriser en temps réel (plutôt que de recourir à des laboratoires d'évaluateurs humains en arrière-plan) avec la capacité de ralentir ou suspendre les fichiers jusqu'à ce que leur téléchargement soit jugé inoffensif. Les NGFW et SWG avaient également recours au sandboxing des fichiers exécutables afin de déterminer les menaces malveillantes puis de mettre à jour les signatures.

Une théorie dominante à cette époque était que plus les membres d'une communauté étaient nombreux, plus grande était l'exposition à de nouvelles menaces par infection du patient zéro, et ainsi plus vite un fournisseur de sécurité pouvait développer et partager de nouvelles signatures.

S'ajoutant aux SWG, l'isolation du navigateur à distance (RBI) fournissait une vue générée en pixels des sites Web et du contenu inconnu et potentiellement malveillant pour protéger les utilisateurs et leurs appareils contre les attaques.

Stratégie de protection contre les menaces au niveau des points de terminaison et passerelles

L'inspection du trafic chiffré à grande échelle et hautes performances a même gagné en importance pour protéger les utilisateurs et les ressources contre les attaques basées sur au niveau des fichiers, sans fichiers et de phishing.

Jusqu'à 2017, et la croissance des menaces sans fichiers, le point de terminaison convenait le mieux pour analyser les menaces exécutables ayant accès au système de fichiers, à l'exécution et au répertoire. Les attaques sans fichiers exécutées en mémoire évitent le système de fichiers en utilisant des scripts d'exécution pour créer un nouvel obstacle. Sans compter que les attaques de phishing portaient sur le contenu sans fichiers exécutables à analyser, et présentaient d'autres manœuvres frauduleuses et ruses pour collecter les accréditations d'accès et tromper les utilisateurs. Les SWG sont devenues un partenaire important en matière de protection contre les menaces au niveau du point de terminaison grâce à leur capacité d'analyser le contenu entre les serveurs d'origine et les utilisateurs en servant de point d'inspection des attaques de l'homme du milieu.

Domination des réseaux privés virtuels (VPN) pour l'accès à distance

Cet environnement sur site a été grandement ébranlé au début de la pandémie.

Les premiers réseaux privés virtuels (VPN) nécessitaient un client géré à une époque où les équipes de gestion des postes de travail, confrontées à des conflits entre de multiples agents de point de terminaison, étaient frustrées par l'utilisation d'un « énième agent ». L'innovation des VPN basés sur SSL/TLS au moyen des navigateurs Web a accéléré l'adoption des VPN qui sont devenus prédominants pour l'accès à distance. À ce stade, moins de 20 % des employés d'une organisation étaient en télétravail, ce qui rendait nécessaire la présence de VPN dans les ressources de l'entreprise. La plupart des employés, des sous-traitants et des collaborateurs accédaient à un bureau principal ou une succursale pour leurs tâches professionnelles en travaillant sur un appareil géré sur un réseau géré par l'entreprise, protégé par un NGFW et dans de nombreux cas, une SWG.

Débuts de l'adoption du SaaS/de l'IaaS

Tandis que les NGFW et SWG présentaient des rôles et cycles de régénération bien définis et des fonctionnalités cohérentes, un monde entièrement nouveau se développait en vue des applications SaaS et des services cloud IaaS.

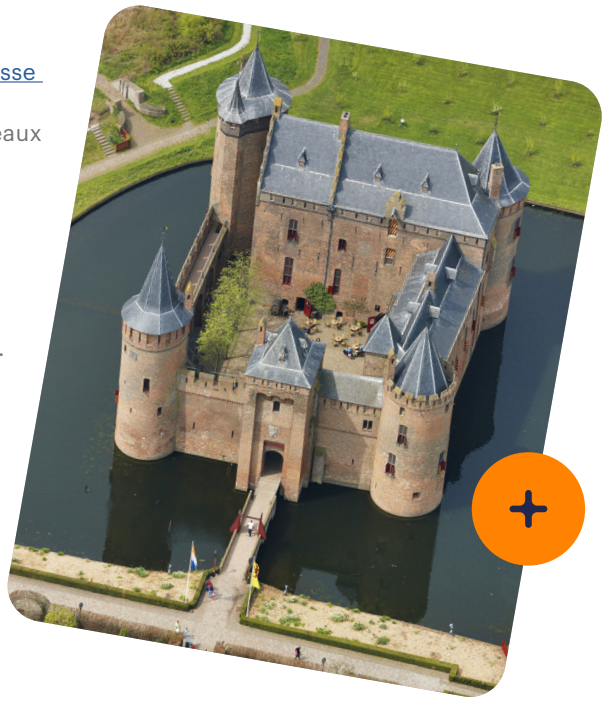
> La plupart des administrateurs des NGFW et des SWG n'ont pas pris en compte ces nouveaux arrivants dans leur domaine de responsabilité et ont ignoré le SaaS et l'IaaS avant la pandémie.

Les solutions CASB (courtier en sécurité d'accès au cloud) étaient axées sur des SaaS et IaaS gérés au moyen d'une inspection API tirant parti des points d'ancrage Web des nouveaux événements ou d'une analyse temporelle. On privilégiait la protection des données et la DLP car les applications SaaS les plus populaires contenaient des données soumises à des réglementations de conformité. Dans un univers parallèle, les utilisateurs étaient également en train d'adopter des applications SaaS personnelles pour leur messagerie, les réseaux sociaux, la messagerie instantanée, les chats, les communications personnelles et le stockage des fichiers dans le cloud. Ces environnements parallèles des SaaS d'entreprise et personnels allaient bientôt se heurter à la pandémie.

Un autre facteur a contribué à créer une véritable tornade au moment de la pandémie. En effet, dans de nombreuses régions du monde, le HTTPS pour le trafic Web chiffré des systèmes d'exploitation et des navigateurs Web a connu une croissance de plus de 90 %. Pour les lignes de défense de sécurité qui ne déchiffrent pas et n'inspectent pas HTTPS, cela a entraîné une augmentation de l'angle mort, une plus grande dépendance vis-à-vis de la communauté des utilisateurs en matière de veille des menaces pour bloquer les menaces connues et une perte de visibilité du mouvement des données à mesure que l'adoption du SaaS/de l'IaaS augmentait. Si vous gériez l'inspection du trafic chiffré et les ressources, vous avez dû constater le quasi-doublement de la capacité requise tous les deux ou trois ans pour faire face à l'utilisation croissante de HTTPS et à l'augmentation du trafic Web et SaaS/IaaS.

Fin de l'ère de la forteresse

Le début des années 2020 a signé la fin de l'ère de la forteresse en matière de défense de sécurité. Les administrateurs de sécurité et de réseau habitués aux utilisateurs dans des bureaux sur leurs réseaux, aux appareils gérés et aux applications et données dans les datacenters allaient bientôt être mis à l'épreuve. Un t-shirt humoristique populaire parmi les administrateurs de cette époque portait le message « Je suis le premier à lire votre mail ». Les TAP réseau pouvaient enregistrer n'importe quel trafic dans des captures de paquets pour le relire et l'analyser, et la visibilité allait de soi.



L'arrivée du télétravail et du travail hybride accentue la transformation numérique

BOUM ! En mars 2020, la pandémie a empêché les travailleurs d'accéder à leurs bureaux, entraînant le plus grand effort de résilience de l'histoire de l'informatique.

Tous les facteurs sont réunis pour créer une crise sans précédent : une capacité VPN limitée, des défenses de sécurité basées sur les datacenters, des angles morts pour l'inspection du trafic chiffré et l'utilisation croissante du SaaS/de l'IaaS.

La pandémie a accéléré le passage des utilisateurs, des applications et des données dans le cloud, au profit de la transformation numérique et de l'agilité des entreprises. Ce qui aurait pu prendre des années pour être adopté s'est produit rapidement et a redéfini les rôles des défenses de sécurité existantes. Les entreprises étaient face à un dilemme : se joindre à la scission numérique ou décrocher, et alors acquérir ou perdre les talents et les compétences informatiques nécessaires à cette évolution.

Les VPN peinent à transmettre le trafic

Dans la foulée, les VPN ont été mis à l'épreuve pour permettre aux télétravailleurs d'accéder aux ressources de l'entreprise et se sont souvent trouvés submergés, jusqu'au déploiement d'une capacité supérieure. Cela a augmenté les coûts ainsi que la complexité, et a ouvert la porte à plus de risques de sécurité. Les VPN utilisaient un port de service public vulnérable, des données d'identification faibles permettaient la compromission des accès et le large mouvement latéral des données d'accès libre ne faisait qu'accroître la surface d'attaque. L'expérience utilisateur de transmission du trafic VPN vers les datacenters via les défenses de sécurité existantes était souvent mauvaise, d'où l'évitement de ce chemin par les utilisateurs ou l'autorisation de leur accès direct au SaaS/à l'IaaS à des fins de productivité. Dans l'un ou l'autre cas, on perdait la visibilité qui allait autrefois de soi.

L'adoption du SaaS s'accélère grâce à une stratégie privilégiant le cloud

L'adoption des applications SaaS gérées augmentait de plus de 18 % année après année, principalement pour les suites bureautiques, la gestion de la relation client, le marketing et les ressources humaines. Simultanément, le SaaS personnel est rapidement devenu une option de résilience pour les effectifs en télétravail, qui pouvaient partager les fichiers, déplacer les données et accomplir leurs tâches avec le moins de friction possible.

Alors que le SaaS géré pouvait utiliser une inspection API, le SaaS non géré et les instances personnelles des applications SaaS populaires sont rapidement devenus un angle mort après la pandémie.

Bien que les équipes de réseau et de sécurité aient maîtrisé pendant plus d'une décennie la gestion des NGFW et des SWG, elles découvraient l'inspection du trafic Web par CASB pour une utilisation professionnelle et personnelle du SaaS et de l'IaaS. Les entreprises adoptant une stratégie privilégiant le cloud étaient confrontées à un nouvel angle mort. Elles ne pouvaient pas détecter le mouvement ou l'exfiltration de données inconnues ou non approuvées.

Les NGFW se divisent en deux catégories : les FWaaS pour la sortie à distance et le ZTNA pour l'accès à distance

Pour les employés en télétravail ou en travail hybride, il y avait peu d'intérêt à transmettre leurs transactions métier aux défenses des datacenters en raison de la mauvaise expérience utilisateur. Pour ces utilisateurs, le rôle du NGFW connaît un changement rapide car le trafic sortant est désormais protégé par un Firewall-as-aService (FWaaS) faisant partie intégrante d'une plateforme de sécurité SSE ainsi que par un proxy combiné pour l'inspection du trafic Web et SaaS/IaaS qui fusionne ensemble la SWG et le CASB au cœur du système. L'accès à distance via les VPN s'est également transformé en un accès au réseau zero trust (ZTNA) basé sur les principes du zero trust au moyen d'une connexion « à l'envers » plus sécurisée. Le rôle traditionnel du NGFW demeure maintenant au sein des datacenters pour le trafic entrant et sortant à moins que l'entreprise ne donne priorité au cloud à 100 % et ne mette ses datacenters hors service. Comme on l'a vu avec les appliances SWG, l'appliance NGFW tend à disparaître à mesure que les cas d'utilisation changent, que le cloud monte en puissance et que les performances des utilisateurs, des appareils et des emplacements prévalent.

Consolidation éclair de la plateforme Security Service Edge

Quelques analystes avaient prédit, avant la pandémie, la consolidation des défenses de sécurité vers des plateformes en périphérie du cloud, et après la pandémie, ils ont rapidement constaté à quel point ils avaient vu juste. Ce qui était au départ un Secure Access Service Edge (SASE) s'est affiné pour donner lieu à un Security Service Edge (SSE) et un SD-WAN. Les fournisseurs de NGFW et de SWG ont été pris au dépourvu : un PDG dans le domaine des SWG a ainsi tenté de s'imaginer comment un fournisseur de CASB pouvait être leader sur le marché des solutions SSE. Le trafic SaaS/IaaS professionnel et personnel dépassait désormais le trafic Web en volume et nécessitait à la fois un déchiffrement TLS et le décodage des applications SaaS/IaaS à des fins de visibilité de contenu. À cette époque, les solutions CASB étaient principalement considérées comme une inspection API du SaaS géré pour la DLP et la conformité.

Aujourd'hui, l'inspection du trafic Web via CASB destinée au trafic SaaS, IaaS et Web professionnel et personnel est un géant qui occupe la première place sur le marché des solutions SSE. Cette nouvelle visibilité post-pandémie a rapidement confirmé que plus de la moitié des menaces provenaient du cloud et non du Web, et que l'exfiltration et le vol de données augmentaient de 300 % au cours des 30 derniers jours de travail des employés qui quittent une entreprise.

> Les cas d'utilisation traditionnels des NGFW et des SWG n'ont pas tenu compte de l'adoption croissante du SaaS et de l'IaaS pour une utilisation professionnelle et personnelle, ni de l'impact de l'accélération de la pandémie.

Bloquer ces domaines ne fait que frustrer les utilisateurs et supprimer potentiellement une option de résilience en cas d'indisponibilité des applications principales. La connaissance des utilisateurs, des applications et du mouvement des données est devenue primordiale et centrale sous l'effet des plateformes SSE, des stratégies privilégiant le cloud et de la transformation numérique. Le rôle des NGFW et des SWG avait changé et devait faire face à un nouvel obstacle.

Les principes du zero trust comparés au marketing

Les principes du zero trust visent à supprimer l'accès implicite, affiner l'accès du moindre privilège et assurer une surveillance continue. À partir de ces concepts de base, le marketing du zero trust reste très éloigné de la réalité. La plupart des messages marketing du zero trust parlent de son accès sécurisé sans préciser que les flux de données traversent toutes ses autres composantes (utilisateurs, applications, appareils et réseaux).

> Les principes du zero trust sont mal adaptés aux angles morts des défenses de sécurité existantes.

Le concept de l'accès du moindre privilège pour une transaction commerciale, basé sur le contenu et le contexte ne fonctionne que si vous avez de la visibilité. Et si vous souhaitez effectuer une surveillance permanente pour affiner l'accès du moindre privilège, vous avez besoin d'une visibilité sur l'utilisateur, les données, l'application, l'appareil et le réseau. De ce fait, les solutions SSE combinent les fonctionnalités des CASB et des SWG en un proxy en ligne de base doté d'un FWaaS et du ZTNA en vue de redéfinir les rôles traditionnels des NGFW et des VPN pour prendre en charge les principes du zero trust. Comme il s'agit d'une plateforme de sécurité cloud en périphérie, la SSE a l'évolutivité et les performances qui conviennent à tout utilisateur, appareil, ou emplacement pour offrir une expérience utilisateur de qualité sans compromis sur les performances ou la sécurité quant à la visibilité du contenu.

Les cybercriminels perfectionnent leurs ransomwares

> Les ransomwares monétisent les accès à distance compromis et reflètent la nécessité d'appliquer les principes du zero trust.

Les entreprises qui se reposaient sur les défenses existantes, notamment les VPN, les solutions prenant en charge l'accès à distance, les pare-feux traditionnels et qui n'étaient pas en mesure de détecter les compromissions d'accès aux comptes, aux utilisateurs et aux appareils étaient devenues des cibles faciles. Si votre première ligne de défense consiste à détecter les ransomwares qui chiffrent les données et gèrent les clés de chiffrement, l'exfiltration des données a déjà eu lieu lors des étapes précédentes de cette chaîne délictuelle et l'extorsion ne manque pas de suivre. Les compromissions d'accès à distance et le phishing sont les principaux points d'entrée des ransomwares et génèrent une économie souterraine multi-sectorielle qui vend l'accès aux cibles visées.

Les réglementations gouvernementales y ont réagi en instaurant des exigences d'authentification forte et multi-facteur, et recommandent en outre de remplacer les solutions VPN susceptibles d'être compromises et vulnérables aux menaces zero-day. Le ZTNA qui utilise une connexion à l'envers spécifique à une application ou une ressource est plus sécurisé, de même que l'utilisation d'adresses IP de sortie dédiées vers les applications SaaS gérées à partir de plateformes SSE. Le phishing requiert une analyse de contenu en temps réel pour le trafic Web, de messagerie, SaaS et IaaS du fait que des formulaires de connexion factices sont souvent hébergés dans des services cloud SaaS et IaaS populaires. Les ransomwares vont continuer à entraîner le remplacement des solutions de sécurité existantes lorsqu'ils seront analysés de manière holistique et au-delà du fichier exécutable malveillant lui-même.

Exfiltration de données inconnues et non approuvées, vol et menaces internes

Au début de la pandémie, les employés ont emporté chez eux leurs appareils gérés pour accéder à une grande variété de contenus non professionnels, sans compter les multiples utilisations d'ordinateurs portables à des fins de formation, personnelles et pour l'accès aux réseaux sociaux. Les contenus réservés aux adultes ont augmenté de plus de 600 % dans un premier temps puis ont décliné. Cela n'était pas surprenant. Lorsque le WiFi est apparu sur les lignes aériennes commerciales, le même phénomène s'est produit et les compagnies l'ont désactivé jusqu'à la mise en place du filtrage du Web. Cette nouvelle expérience de travail à distance a également donné lieu à des changements sur le plan de l'emploi et de l'activité professionnelle, certaines personnes souhaitant conserver cette pratique à long terme. Certaines sociétés informatiques ont même eu la bonne idée de publier des annonces en télétravail illimité afin d'attirer les talents d'autres entreprises qui leur demandaient de retourner au bureau.

Ce que les employés font sur leur ordinateur au bureau sous les yeux de leurs collègues et ce qu'ils font à distance sont deux choses différentes. L'exposition à plus de contenus non professionnels ouvre la porte à un plus grand nombre de leurres et de menaces.

> Les employés, les sous-traitants et les partenaires s'approprient plus facilement les données qu'ils voient comme des atouts pour leurs emplois futurs.

C'est ce qu'a montré l'augmentation de 300 % des exfiltrations et des vols de données au cours des 30 derniers jours qui précèdent le départ d'un employé, 74 % de ces données étant conservées dans un espace de stockage personnel sur le cloud L'exfiltration de données inconnues et non approuvées, le vol et les menaces internes ont augmenté avec le travail hybride/le télétravail là où, les défenses existantes ne distinguaient pas les utilisations professionnelle et personnelle du SaaS et de l'IaaS. Les solutions NGFW et SWG n'étaient pas préparées à cet environnement où moins de 3 % des applications SaaS étaient gérées par le service informatique et qui voyait l'adoption des 97 % restants par les unités commerciales et les utilisateurs passant à la transformation numérique.

Le contrôle d'accès adaptatif en temps réel reposera à l'avenir sur le contenu et le contexte

L'inspection en ligne du contenu et du contexte SaaS et IaaS en temps réel est l'avenir en matière de contrôle d'accès pour les SSE. Les pare-feux ont perfectionné l'inspection du trafic réseau, les SWG ont fait la même chose pour le trafic Web et les solutions SSE associent ces types de contrôles à une inspection basée sur le contenu et le contexte via un CASB en ligne. Selon le risque lié à l'application, le risque lié à comportement, la posture de l'appareil, l'activité, la sensibilité des données et d'autres variables, un contrôle d'accès adaptatif est appliqué à chaque transaction de l'entreprise selon son contenu et son contexte. Si un utilisateur souhaite supprimer 100 fichiers de données sensibles de l'entreprise, l'accès adaptatif peut demander une authentification renforcée ou une justification à l'utilisateur.

> Nous nous trouvons dans une nouvelle zone grise entre ce que nous connaissons de bon et de mauvais, qui requiert un accès adaptatif et des directives pour que les utilisateurs et les données soient protégés.

Si un autre utilisateur souhaite accéder à une application de stockage cloud risquée et non gérée, l'accès adaptatif peut l'avertir et proposer des options de stockage cloud plus sûres et approuvées par l'entreprise. Le concept d'accompagnement en temps réel peut se comparer à la conduite avec la navigation satellite (ou GPS) : les utilisateurs ont besoin d'être guidés en temps réel.

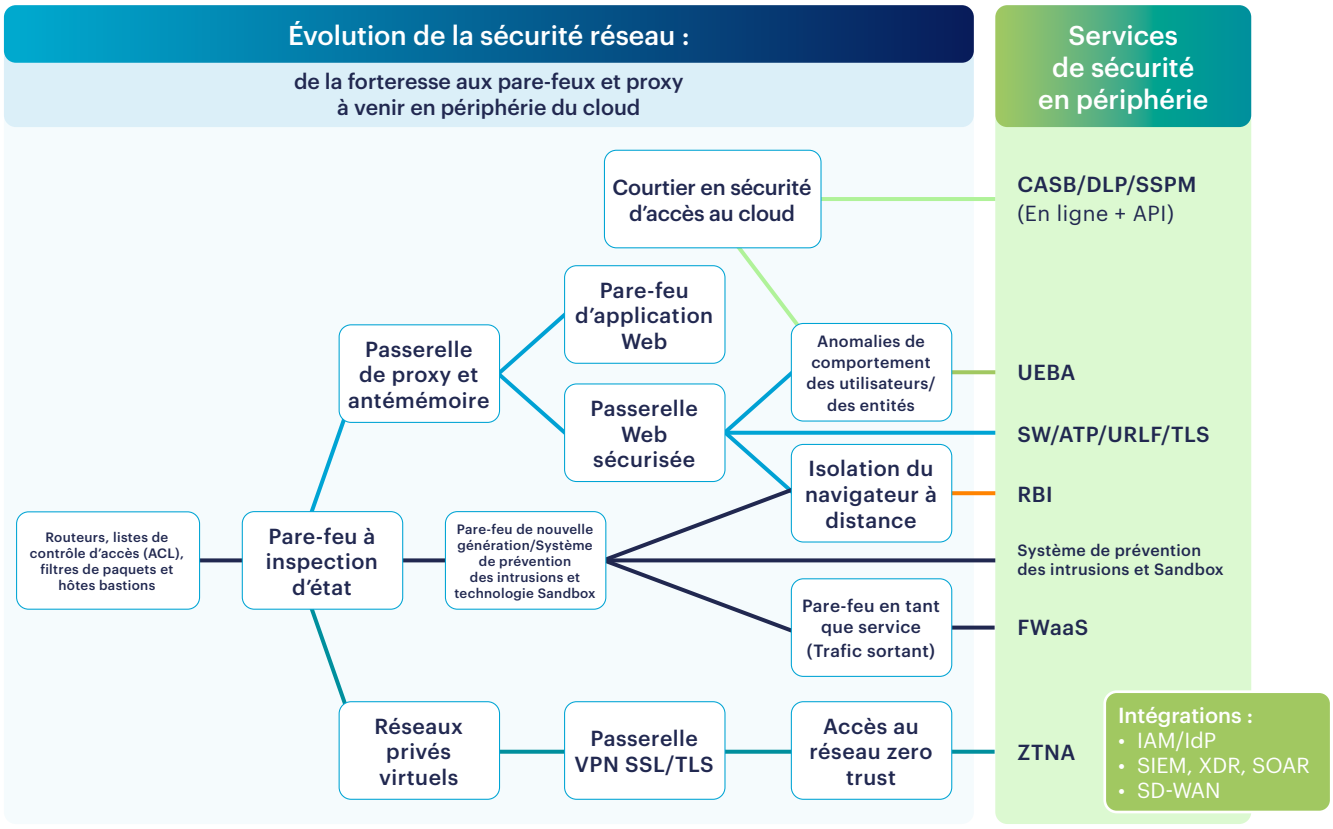
Rôle de l'IA et de l'apprentissage automatique pour la protection des données et contre les menaces

Depuis de nombreuses années, l'intelligence artificielle (IA) et l'apprentissage automatique (AA) ont été utilisés en arrière-plan pour les moteurs de défense contre les menaces, la classification des données, la notation dynamique des URL et la planification des opérations informatiques, pour ne citer que quelques exemples. Les défenses reposant sur l'IA et l'AA se déploient désormais en ligne pour fonctionner en temps réel afin de détecter les nouvelles menaces zero-day inconnues et d'identifier les données sensibles dans les documents et les images. L'essor de l'IA permet aux acteurs, bienveillants ou non, de développer rapidement du nouveau code et de nouveaux contenus et d'apprendre rapidement. L'IA représente un formidable potentiel mais peut aussi tromper et entraîner l'exposition de données sensibles. ChatGPT est devenu rapidement la première application d'IA accessible et le contenu le plus populaire qui lui a été transmis était du code source. Les défenses existantes n'étaient pas en mesure d'autoriser les instances d'IA au sein de l'entreprise, ni de contrôler les instances personnelles et publiques pour les utilisateurs, ni de permettre d'identifier un contenu tel que du code source fourni aux applications d'IA. Les lignes de défense basées sur l'IA/AA détectent les fichiers exécutables malveillants, les attaques de phishing et classent des dizaines de documents et d'images, y compris aujourd'hui du code source.

> Les lignes de défense IA/AA assurant une protection en temps réel à T+0 ne fonctionnent que si le contenu est visible, et c'est le rôle d'une plateforme SSE moderne.

Utilisations modernes des NGFW, SWG, CASB, VPN et ZTNA dans le cadre du zero trust

Pour le trafic Web, la passerelle Web a vite scindé ses fonctions, le trafic sortant étant géré par la SWG et le trafic entrant par le WAF. Bien que le NGFW ait continué à associer les trafics réseau entrant et sortant, le flux de trafic sortant post-pandémie traverse le FWaaS pour les employés en travail hybride ou en télétravail, et les fonctionnalités VPN sont remplacées par le ZTNA au sein des plateformes SSE. À ses débuts, le CASB se définissait principalement par une inspection API des SaaS et IaaS gérés avec une DLP pour les données au repos. La fonctionnalité de ligne de défense souvent ignorée du CASB qui permet d'inspecter des milliers d'applications et services cloud gérés et non gérés, notamment au moyen d'une instance de l'entreprise ou personnelle pour des centaines d'applications, est vite devenue hautement prisée. Les principes du zero trust et l'intérêt croissant qu'ils suscitent requièrent une visibilité du contenu et du contexte pour l'accès du moindre privilège et la surveillance continue de chaque transaction de l'entreprise. Ces mêmes contenu et contexte seront les moteurs de l'évolution future des défenses IA/AA en temps réel au sein des plateformes SSE.



SYNTHÈSE

Investir dans des défenses de sécurité pour une infrastructure qui n'existe plus ou qui va bientôt disparaître est une erreur coûteuse dans le contexte de l'adoption croissante du travail hybride et de la transformation numérique. Il convient d'analyser minutieusement les renouvellements des NGFW, SWG et VPN en tenant compte du passage vers une inspection en ligne SaaS et IaaS, de la visibilité du contenu pour les lignes de défense IA/AA et de la fourniture d'un accès adaptatif avec un accompagnement en temps réel des utilisateurs.

> Il est important pour chacun de savoir comment nous en sommes arrivés là et de connaître les moteurs du changement en matière de trafic réseau, Web et SaaS/IaaS entrant et sortant.

Les esprits novateurs et les adeptes de la première heure s'adaptent rapidement en constatant les signes de changement à mesure qu'ils favorisent l'innovation, qu'ils établissent des feuilles de route et valident les prévisions des analystes. Pour la majorité d'entre nous, la vitesse à laquelle nous reconnaîtrons les technologies post-pandémie et nous y adapterons déterminera notre réussite, les talents du secteur informatique que nous attirerons et retiendrons et notre capacité à nous préparer aux changements à venir. Dans tous les aspects de notre vie, force est de constater que la technologie avance en dépit de toutes les résistances humaines face au changement.

POURQUOI NETSKOPE

La plateforme Netskope Intelligent SSE offre des fonctionnalités exceptionnelles pour l'inspection du trafic Web, SaaS et IaaS de milliers d'applications et de services cloud afin d'en connaître le contenu et le contexte. Son architecture de base comprend le ZTNA pour l'accès aux applications privées et l'intégration complète des solutions SWG et CASB pour une inspection single pass du trafic en ligne provenant des utilisateurs ou des systèmes. Cette visibilité détaillée permet au moteur Netskope Zero Trust Engine de fournir des contrôles d'accès adaptatifs, un accompagnement en temps réel et une connaissance des instances d'entreprise et personnelles de centaines d'applications afin de détecter les mouvements de données inconnus. Grâce à l'accès du moindre privilège, les utilisateurs ont la possibilité de fournir des justifications pour continuer leurs transactions commerciales, et les règles sont affinées par une surveillance continue prenant en charge les principes du zero trust.

Pour en savoir plus, lisez notre eBook **Nouvelles perspectives pour la protection des données et la protection contre les menaces — Ce que les fournisseurs traditionnels veulent cacher**, enotre infographie, et suivez notre webinaire à la demande.

Netskope, leader mondial du SASE, redéfinit la sécurité du cloud, des données et des réseaux pour aider les organisations à protéger leurs données en appliquant les principes du zero trust. Rapide et simple à utiliser, la plateforme de Netskope offre un accès optimisé et une sécurité en temps réel pour les personnes, les appareils et les données, où qu'ils se trouvent. Netskope aide ses clients à réduire les risques, à accélérer les performances et à obtenir une visibilité inégalée sur l'ensemble des activités des applications cloud, Web et privées. Des milliers de clients, dont plus de 25 entreprises figurant au classement Fortune 100, font confiance à Netskope et à son puissant réseau NewEdge pour faire face aux menaces toujours grandissantes, mais aussi aux risques émergents, à l'évolution technologique, aux révolutions organisationnelles et réseau, ainsi qu'aux nouvelles exigences réglementaires.

Pour savoir comment Netskope aide ses clients à répondre à toute menace dans leur parcours SASE, consultez le site netskope.com.