Akamai

LIVRE BLANC

Modèle d'adoption d'une architecture Zero Trust Network Access

Qui doit lire ce guide ?

Les architectes réseau, les ingénieurs en sécurité, les directeurs techniques, les RSSI et les autres décideurs informatiques et de sécurité profiteront tous de la lecture de ce guide.

Pour les personnes responsables de la détermination de la portée, de la configuration, du déploiement, de la mise en œuvre et de la gestion d'un projet ZTNA (Zero Trust Network Access), ce guide fournit un examen complet des avantages potentiels et des différences entre les différents systèmes. Ce guide présente :

- les limitations et les failles de sécurité des approches héritées de l'accès aux applications et les raisons pour lesquelles le ZTNA est nécessaire ;
- les composants du ZTNA et son fonctionnement ;
- la façon dont Enterprise Application Access d'Akamai et Akamai MFA peuvent fournir un ZTNA rapidement et facilement.

À mesure que le monde des affaires évolue et que les cybermenaces s'intensifient, les entreprises portent un regard neuf sur leurs cyberdéfenses. Nombreuses sont celles qui se sont rendu compte que l'architecture réseau traditionnelle, reposant sur un emplacement centralisé où les applications sont accessibles à toutes les parties, les rendait vulnérables. Cette approche de la sécurité de type « château fort », qui protège le périmètre tout en supposant que tout le monde y est en sécurité, expose les entreprises au risque de cyberattaques dans le paysage actuel des connexions mobiles et du cloud. Les entreprises à la pointe de la technologie se tournent donc vers un concept d'architecture Zero Trust pour protéger leurs actifs vitaux. Un principe fondamental de tout projet Zero Trust est la protection du réseau. Ce livre blanc explique en quoi les approches traditionnelles de la sécurité réseau en étoile ne sont plus suffisantes et comment le passage au ZTNA permet de mieux défendre les actifs critiques et peut être un rouage clé dans l'optique d'une architecture Zero Trust complète.

Les entreprises n'ont jamais vécu de changement aussi rapide

La façon dont les entreprises fonctionnent et utilisent la technologie évolue à un rythme toujours plus rapide. L'évolution de l'informatique a entraîné une transition rapide de l'hébergement d'applications métier. Les centres de données sur site ont laissé la place à différents clouds publics et clouds privés, ou à une approche hybride (à la fois sur site et dans le cloud public/privé).

L'évolution du modèle économique a également stimulé la collaboration entre les entités et la nécessité de fournir aux partenaires et aux fournisseurs un accès aux applications et aux ressources.

Enfin, alors que les entreprises continuent d'adopter le travail à distance ou hybride, les utilisateurs accèdent désormais aux applications et ressources de l'entreprise depuis n'importe où, sur des terminaux gérés et non gérés.

Avec ces changements, les approches héritées de la gestion de l'accès aux applications ne suffisent plus et les entreprises doivent désormais adopter une nouvelle approche permettant un accès sécurisé, quel que soit l'endroit où les applications sont hébergées ou celui où se trouvent les utilisateurs.

Accès aux applications existantes

Depuis plus de 20 ans, les entreprises comptent sur les pare-feux pour construire un périmètre de sécurité solide et font confiance aux utilisateurs qui se trouvent à l'intérieur de ce périmètre. Cela équivaut à traiter les réseaux comme des châteaux forts : des murs épais et des portes hautement sécurisées forment un périmètre pour protéger le château (ou, dans le cas présent, le réseau) et seuls les utilisateurs ayant les bonnes informations d'identification sont autorisés à y accéder. Une fois à l'intérieur, les utilisateurs peuvent accéder à des applications spécifiques en fonction de leur identité, fournie par des solutions de fournisseur d'identité (IdP) telles que Microsoft Active Directory.

Cependant, avec les réseaux plats, les utilisateurs ont un accès IP à l'ensemble du réseau, ce qui leur permet de découvrir d'autres serveurs et applications. Par exemple, si l'IdP est configuré correctement, un utilisateur peut trouver le serveur sur lequel l'application de paie est hébergée, mais lorsqu'il tente de s'y connecter, il se verra refuser l'accès.

Pour résoudre ce problème de mouvement latéral illimité, les entreprises ont partitionné les applications via des réseaux d'accès locaux virtuels (VLAN) en segments séparés derrière un pare-feu et ont appliqué des règles désormais archaïques reposant sur la plage IP pour des utilisateurs individuels ou des groupes. Ce processus constitue une solution précaire et source d'erreurs. Imaginez un scénario dans lequel des coupures peuvent survenir pour des raisons de maintenance et de déplacement des machines vers de nouveaux racks, ou encore lorsqu'une nouvelle plage IP leur est attribuée. Soudain, les utilisateurs perdent leur accès et les appels au service d'assistance s'accumulent. Il se peut également qu'une mise à niveau logicielle nécessite des modifications de l'architecture d'une application et que les utilisateurs soient redirigés vers une autre machine dans le cadre du flux de travail. Cette machine peut alors être inaccessible à certains utilisateurs ou groupes, car les règles du pare-feu n'ont pas été mises à jour.

Cette architecture est excessivement complexe et exige un niveau de communication élevé entre les propriétaires d'applications, les administrateurs de réseau et les groupes de sécurité pendant les modifications, afin de garantir l'absence complète d'interruption.

Nous savons ce qui se produit souvent lorsque cette coordination échoue. Les administrateurs veulent suivre les meilleures pratiques, mais dans les moments de désespoir, ils ajoutent la redoutable règle IP ANY/ANY ALLOW comme solution rapide pour permettre aux utilisateurs concernés de conserver leur accès jusqu'à ce que le problème soit diagnostiqué et résolu. Souvent, le temps manque pour revenir en arrière et annuler ces changements, et ces correctifs rapides amoindrissent la posture de sécurité d'une entreprise au fil du temps.

Les VPN ajoutent des difficultés en matière de complexité, de performances et de sécurité

Pour les utilisateurs distants, un réseau privé virtuel (VPN) fournit généralement un accès aux applications sur site hébergées à l'intérieur du périmètre, qui fournissent ensuite un accès direct par tunnel au réseau de l'entreprise.

Pour gérer l'accès des utilisateurs aux applications, les entreprises ajoutent souvent des contrôleurs de diffusion d'applications dédiés ou utilisent les contrôles d'accès intégrés à leurs solutions VPN. L'objectif est d'aligner les autorisations d'accès aux applications, quel que soit l'emplacement de l'utilisateur. Si un utilisateur se voit refuser l'accès à l'application de gestion de la relation client lorsqu'il se trouve à l'intérieur du périmètre, il devrait se voir refuser l'accès lorsqu'il est connecté via le VPN. Bien que ce soit l'objectif, en réalité la complexité de la synchronisation des autorisations d'application entre les deux cas d'utilisation, ainsi que les correctifs rapides, peuvent conduire les utilisateurs à obtenir un accès involontaire aux applications.

Accès aux applications pour les sous-traitants, partenaires et fournisseurs

Les entreprises utilisent également souvent des VPN pour permettre aux sous-traitants, aux entreprises partenaires ou aux fournisseurs d'accéder à distance à leurs applications. Par exemple, une entreprise peut autoriser un accès externe à ses systèmes financiers pour permettre à ses fournisseurs de soumettre des factures. Autoriser l'accès à des applications tierces via un VPN introduit des risques de sécurité supplémentaires, car l'entreprise ne détient plus la sécurité de bout en bout. Si un terminal tiers doté d'un accès VPN est compromis, les cybercriminels peuvent accéder au réseau de l'entreprise.

VPN et performances

Le même compromis se produit au niveau des performances. Avec un VPN dans sa forme la plus simple, le trafic est redirigé vers l'infrastructure du centre de données. Cela peut entraîner un accès extrêmement lent aux ressources Internet et aux applications SaaS (Software-as-a-service) en raison du hairpinning, qui double le trafic.

Pour relever ce défi de performance, les administrateurs déploient généralement des tunnels partagés, en distinguant de nouveau les plages IP devant revenir vers le VPN de celles qui doivent conduire directement à Internet. Il s'agit d'une solution qui peut être simple et efficace lorsque vous disposez d'un seul périmètre interne. Cependant, les choses se compliquent en cas d'ajout de plusieurs fournisseurs de centres de données et de cloud privé virtuel. Les administrateurs doivent alors déterminer s'ils souhaitent installer des agrégateurs VPN dans chaque centre de données et comment ils vont gérer efficacement les tunnels partagés multipoints.

Il ne s'agit pas de prétendre que les VPN n'apportent pas de valeur. Loin de là, en réalité. Les VPN s'avèrent particulièrement utiles pour les accès de site à site dans les infrastructures comptant plusieurs centres de données. Cependant, l'accès au niveau du réseau n'est pas le bon paradigme pour les utilisateurs qui accèdent aux applications, car ce type d'accès impose un compromis contre nature entre simplicité et sécurité/performances.

L'accès aux applications réseau est une aubaine pour les cybercriminels

Jusqu'à présent, nous nous sommes concentrés sur les risques et les défis associés à l'octroi d'un accès au niveau du réseau à tous les collaborateurs. Cependant, cette approche expose également les entreprises à un autre risque : les cybercriminels qui exploitent des informations d'identification d'utilisateur volées ou une faille de sécurité ont également la possibilité d'obtenir un accès illimité à l'ensemble du réseau. Par exemple, si un pirate obtient un accès VPN à l'aide d'informations d'identification compromises, il peut alors se déplacer latéralement sur le réseau pour trouver des cibles de grande valeur, y accéder et les attaquer.

Ces approches augmentent la probabilité d'une violation de sécurité aux conséquences catastrophiques

Il est théoriquement possible de gérer l'accès aux applications en toute sécurité et avec un minimum de friction en utilisant ces approches. Vous utilisez peut-être déjà une combinaison d'entre elles. Le problème, c'est que les mettre en œuvre correctement et garantir de bonnes performances ainsi qu'une sécurité robuste pendant leur durée de vie est souvent bien trop complexe pour assurer une efficacité permanente. Les entreprises considèrent souvent qu'il n'y a aucun problème tant que leurs employés peuvent accéder à leurs applications. Elles sont alors prises au dépourvu lorsque l'une de ces corrections rapides donne lieu à une défaillance catastrophique ou dégrade suffisamment les performances pour entraîner une panne ou limiter significativement la productivité des employés.

Une approche Zero Trust de l'accès aux applications

Compte tenu des failles inhérentes aux approches de sécurité périmétrique et des défis spécifiques qu'elles présentent dans la gestion de l'accès aux applications, le modèle de cybersécurité émergent Zero Trust constitue une meilleure alternative. Introduit pour la première fois par Forrester Research en 2010, il s'agit d'un cadre de sécurité que les entreprises utilisent pour transformer leur infrastructure informatique, leurs stratégies de sécurité et leurs processus métier.

Aussi simple soit-il, ce principe est redoutable : la confiance n'est pas une affaire d'emplacement. Vous n'avez aucune raison d'accorder votre confiance à un individu ou système sous prétexte qu'il se trouve derrière votre pare-feu. Toute action, quel que soit l'endroit où elle se produit, ne devrait bénéficier de la confiance que si elle a été explicitement autorisée. En fin de compte, seul ce qui *doit* se produire *peut* se produire. Supprimez toute confiance implicite pour les actions qui ne sont pas requises, car elles créent des risques mais n'apportent aucune valeur.

Cela nécessite une authentification et une autorisation fortes, et les systèmes ne doivent pas transférer de données tant que la confiance n'a pas été établie. En outre, des mesures d'analyse, de filtrage et d'enregistrement doivent être mises en œuvre pour vérifier les comportements et constamment guetter les signes de dangers éventuels.

Ce changement fondamental permet de contrer une grande partie des types de compromissions de la sécurité observées ces dix dernières années. Les pirates informatiques ne peuvent plus tirer profit de vos failles pour franchir votre périmètre, puis récolter vos données ou applications sensibles une fois à l'intérieur de celui-ci. Il n'y a plus de douves ou de forteresse à franchir pour obtenir l'accès. Tout se résume désormais à des applications et des utilisateurs, qui doivent montrer patte blanche avant de bénéficier de droits d'accès.

Zero Trust Network Access

Le ZTNA est une architecture construite sur ces principes : elle accorde un accès sécurisé aux applications et aux ressources sur la base d'une authentification forte, d'une autorisation et du contexte. Une architecture ZTNA permet d'accéder uniquement aux applications dont les utilisateurs ont besoin pour accomplir leur travail, et non à l'ensemble du réseau. Avec une approche ZTNA, l'emplacement des utilisateurs n'a plus d'importance ; il n'y a plus de concept d'intérieur ou d'extérieur du périmètre. Le site d'hébergement d'une application n'est pas pertinent, que ce soit sur site, dans un cloud public ou dans un cloud privé, car les utilisateurs authentifiés n'ont accès qu'aux applications qu'ils ont été autorisés à utiliser.

Par exemple, un commercial n'aura accès qu'aux applications liées à son poste, et non aux applications de ressources humaines ou financières.

Fonctionnement du ZTNA d'Akamai

Enterprise Application Access d'Akamai et Akamai MFA vous permettent de passer à une architecture ZTNA, ce qui peut être une étape importante et critique dans votre transition vers le Zero Trust.

Enterprise Application Access est un IAP (Identity Aware Proxy) dans le cloud. Il s'agit d'un service flexible et adaptable avec une prise de décision détaillée basée sur des signaux en temps réel, tels que les renseignements sur les menaces, le profil des terminaux et les identifiants utilisateur. Akamai MFA est un service d'authentification multifacteur qui fournit les niveaux d'authentification les plus élevés pour garantir qu'un utilisateur demandant l'accès est bien qui il prétend être.

Pour commencer, vous exécutez une petite machine virtuelle : le connecteur Enterprise Application Access, situé derrière le pare-feu, mais avec une connectivité à vos applications. Cette machine virtuelle ne nécessite *pas* d'être placée dans votre zone démilitarisée (DMZ). Son adresse doit se trouver sur un espace IP privé et ne pas être accessible sur Internet. Elle doit en fait se présenter comme toute autre application à placer derrière le pare-feu.

Pour prendre en charge les environnements multicloud, un connecteur peut être déployé dans votre centre de données sur site ou dans un cloud privé ou public.

Le connecteur Enterprise Application Access établit immédiatement une connexion chiffrée sortante vers l'IAP sur Akamai Connected Cloud. Une fois connecté à l'IAP, le connecteur télécharge sa configuration et est prêt à fournir les connexions. La connexion entre le connecteur et l'IAP est sortante, ce qui vous permet de fermer toutes les connexions entrantes du pare-feu et ce qui rend les applications presque invisibles sur l'Internet public.

L'IAP effectue tout le pré-traitement qui se produit avant qu'un utilisateur ne soit connecté à l'application, y compris l'authentification, l'autorisation, la sécurité des terminaux et les vérifications de profil. Lorsqu'un utilisateur tente d'accéder à une application, il est dirigé vers Akamai par le biais d'un DNS CNAME et se connecte à l'IAP. En supposant que votre utilisateur final et son terminal passent tous les contrôles, ils sont ensuite acheminés pour l'authentification, l'authentification multifactorielle et l'authentification unique, puis les fonctions d'identité du terminal sont exécutées.

Une fois l'utilisateur et sa machine autorisés, la connexion de l'utilisateur final est adjointe à la connexion sortante du connecteur Enterprise Application Access. Le trafic provenant de la session utilisateur transite par cet IAP combiné, qui se connecte alors à l'application ou au service demandés. À ce stade, un chemin d'accès aux données complet est créé. Toutes les décisions relatives aux accès sont appliquées de manière continue et dynamique sur la base de l'identité, du terminal et du contexte utilisateur.

Cette méthode d'accès présente des avantages significatifs. Les activités les plus sensibles aux performances et à la sécurité s'effectuent en bordure de l'Internet, à proximité de l'utilisateur final, où Akamai possède plus de 4 200 sites à travers 134 pays.

En outre, la voie d'intégration sensible à l'application passe par un tunnel d'application inversé qui masque l'adresse IP du périmètre et réduit les risques d'exposition aux attaques volumétriques.

Enterprise Application Access peut s'intégrer directement à l'infrastructure d'identité d'une entreprise, même si elle utilise plusieurs annuaires et fournisseurs de services d'identité ; le service ZTNA peut donc être déployé rapidement sans avoir à modifier l'infrastructure ou l'architecture d'identité existante.

Pour les applications héritées qui ne prennent pas en charge les protocoles d'authentification actuels, Enterprise Application Access dispose d'une fonctionnalité de pont IDP qui fournit une authentification aux IdP SAML et convertit le jeton d'authentification en protocole d'authentification pris en charge par les applications héritées.

Si les approches basées sur des IAP, telles qu'Enterprise Application Access, sont si intéressantes, c'est parce qu'elles proposent un accès au niveau des applications. Avec un accès au niveau des applications, les performances et la sécurité *ne sont plus* synonymes de complexité.

Il vous suffit de prendre toutes les applications partageant le même emplacement (hébergées dans le même centre de données ou le même cloud privé virtuel, par exemple), de les intégrer à l'espace IP d'un réseau privé ou à un réseau LAN virtuel (VLAN) à accès restreint, puis de placer un proxy d'accès dans ce micro-périmètre. Aucune autre opération n'est nécessaire.

Les propriétaires d'applications peuvent définir leurs propres règles de sécurité sur le proxy d'accès (qui peut y accéder et pourquoi) et, de manière encore plus significative, permettre aux utilisateurs de se connecter de partout. Il n'existe aucune distinction entre les utilisateurs sur et hors site, car aucun périmètre réseau n'inclut les utilisateurs finaux. Un collaborateur travaillant dans un café et un employé travaillant dans votre bureau disposent ainsi du même accès. Tout ce qui compte, c'est de savoir si l'utilisateur est autorisé et si son ordinateur est sécurisé.

Avec un accès au niveau des applications, vous obtenez des performances optimales, malgré une utilisation et un déploiement simplifiés. Les utilisateurs passent par Internet pour accéder directement aux applications, indépendamment de leur type d'hébergement ou de leur localisation. Il est ainsi possible d'acheminer des paquets à leur destination sur Internet, sans recourir à des agrégateurs ou à des intermédiaires extérieurs à leur chemin d'accès.

De fait, avec l'accès au niveau des applications, les réseaux internes se fondent souvent parmi les simples réseaux Wi-Fi publics. Gardez bien à l'esprit ce point : pour que le Zero Trust soit réellement efficace, vous ne pouvez faire aucune distinction entre les utilisateurs internes et les utilisateurs externes. Aucun utilisateur n'est approuvé par défaut.

Objectif final du ZTNA

Tous les utilisateurs, qu'ils soient sur site ou hors site, doivent être tenus d'accéder à toutes les applications via des proxys d'accès sensibles à l'identité, quel que soit l'endroit où les applications sont hébergées. Ces proxys doivent non seulement effectuer une authentification standard, mais également une authentification multifactorielle anti-hameçonnage, telle qu'Akamai MFA. En outre, de solides capacités de profils de terminaux doivent être mises en place pour obtenir des critères de terminal et permettre l'accès à des applications spécifiques.

Nous sommes convaincus que le ZTNA ne s'arrête pas à l'authentification et aux autorisations. Pour prendre en charge les principes du Zero Trust, tous les paramètres vérifiés lors de l'authentification et de l'autorisation initiales doivent être surveillés en permanence pendant la session d'activation. Toute modification détectée doit déclencher une action, par exemple, une nouvelle authentification de l'utilisateur ou encore la suppression ou la limitation de l'accès à l'application.

Un système de sécurité crucial devrait être superposé à vos proxys d'accès : la protection des applications Web et des API (WAAP), qui garantit que les utilisateurs finaux ne lancent pas d'attaques au niveau des applications (intentionnellement ou par inadvertance) contre vos applications internes. Vous pouvez profiter d'autres systèmes avancés, comme la détection d'utilisateurs humains/de bots pour les sites hors API, afin de vérifier qu'aucun point de terminaison légitime ne dissimule un logiciel malveillant. C'est au niveau de l'IAP qu'Akamai peut superposer la WAAP, la détection des bots, l'analyse comportementale et la mise en cache. Ces fonctionnalités sont conçues pour fournir des performances optimales, ainsi que pour être en mesure de tenir les potentiels acteurs malveillants à l'écart de vos sites physiques, applications et données.

Lorsque vous mettez vos applications en ligne et les rendez accessibles par le biais de proxys d'accès, la prévention des attaques par déni de service distribué (DDoS) prend encore plus d'importance. Vous devez vous accorder avec des fournisseurs capables d'absorber des attaques visant vos micropérimètres et proxys d'accès, afin d'assurer un fonctionnement continu, y compris en cas de charges massives.

Enfin, pour garantir des performances de pointe pour vos applications et veiller à ce que les utilisateurs adhèrent pleinement à cette nouvelle approche, vos proxys d'accès doivent être gérés par des réseaux capables de leur procurer des avantages en matière de performances. Plus précisément, les réseaux de diffusion de contenu et superpositions de routage Internet doivent faire partie de votre arsenal pour le rendre plus accessible, mais aussi plus performant que toute autre méthodologie ne l'a jamais permis.

Protection contre les menaces

Des solutions comme Akamai Enterprise Application Access peuvent protéger vos applications contre les acteurs malveillants. Mais qu'en est-il de la protection des utilisateurs contre le risque de devenir, par inadvertance, ces mêmes acteurs par le biais d'un compromis, par exemple un terminal infecté par un logiciel malveillant ou des informations d'identification volées via un lien de phishing et une page de renvoi ? C'est là qu'intervient la nécessité d'appliquer des mesures de prévention et de détection au trafic Web.

L'une des approches consiste à déployer une solution de pare-feu DNS reposant sur le cloud, telle que Secure Internet Access d'Akamai. Ce produit inspecte toutes les requêtes DNS émises par les utilisateurs et applique des informations en temps réel sur les menaces afin que les requêtes bénignes soient résolues normalement, mais que toutes les requêtes vers des domaines malveillants soient bloquées de manière proactive. Cela réduit les risques que les terminaux des employés soient compromis par des logiciels malveillants ou des ransomwares, ou soient victimes d'une attaque par hameçonnage.

Résumé

Les architectures classiques de réseaux en étoile, ainsi que les périmètres de sécurité de type « château fort », ne peuvent fournir aucune garantie de performances ou de sécurité dans le monde du cloud et des appareils mobiles d'aujourd'hui. C'est un problème sur lequel toutes les entreprises doivent se pencher, sous peine d'être vulnérables. L'absence d'architectures de sécurité d'entreprise sûres est la principale cause des violations de données des entreprises actuelles, et le nombre de ces violations ne fera qu'augmenter. Pour résumer, le périmètre ne vous protège pas, pour la bonne et simple raison qu'il n'existe plus.

Étapes suivantes

Comment commencer la transition vers une architecture Zero Trust Network Access ?

Les services de sécurité cloud d'Akamai peuvent être combinés pour constituer une architecture ZTNA complète, offrant un accès sécurisé aux applications dans l'univers multicloud, tout en tirant parti de celui-ci pour rendre presque entièrement superflus les réseaux d'entreprise internes.

En utilisant notre IAP distribué avancé et notre authentification multifactorielle anti-hameçonnage, combinés à la puissance d'Akamai Connected Cloud, vous pouvez enfin passer à un monde sans périmètre en toute simplicité, en procédant à la mise en œuvre des applications. Vous pourrez ainsi supprimer presque entièrement les risques liés à la migration et bénéficier de l'expérience d'Akamai en matière de création et de gestion de solutions éprouvées d'optimisation des performances et de la sécurité.

Alors que vous avancez dans votre transition Zero Trust, vous pouvez être sûr qu'Akamai vous accompagnera à chaque étape, vous aidant à réaliser la transition de votre réseau vers une architecture qui, en plus d'offrir un accès à vos applications et données, est facile à gérer et garantit des niveaux de sécurité et de performance supérieurs.

Découvrez comment répondre aux besoins de votre entreprise grâce au portefeuille de solutions Zero Trust d'Akamai.