Guide de l'architecte réseau pour l'adoption d'un service Zero Trust Network Access

Bonnes pratiques pour utiliser ZTNA en tant qu'alternative au VPN

zscaler™

Avec les applications privées qui migrent vers le cloud et l'essor du télétravail, les entreprises ont besoin d'un service qui puisse garantir un accès sécurisé aux applications privées tout en assurant une expérience utilisateur fluide. Malgré le battage médiatique qui entoure la sécurité Zero Trust, certaines entreprises tentent toujours d'utiliser les architectures traditionnelles centrées sur le réseau, qui reposent sur des pare-feu de nouvelle génération conçus pour l'accès au réseau, comme un moyen de limiter la connectivité des utilisateurs aux applications. Ces architectures classiques sont inadaptées aux besoins modernes et n'ont pas été conçues pour connecter des utilisateurs autorisés à des applications spécifiques. Elles obligent les utilisateurs à se placer sur le réseau et entraînent souvent un risque de déplacement latéral vers d'autres applications. Elles exposent également les adresses IP à Internet et aux attaques DDoS via des concentrateurs VPN situés à la périphérie du réseau qui guettent les pings entrants.

De nombreuses entreprises considèrent les services d'accès réseau Zero Trust (ZTNA) comme une alternative au VPN. En effet, Gartner estimait en 2021 que 60 % des entreprises auraient abandonné leur VPN pour un service ZTNA. Mais il s'avère que dans toute grande entreprise (internationale), le moindre petit changement dans la façon dont les utilisateurs accèdent aux applications peut représenter un travail énorme. Ce document vous aidera à comprendre par où commencer pour adopter le ZTNA, rapidement et sans interrompre votre activité.

Dans ce guide, nous aborderons les points suivants :

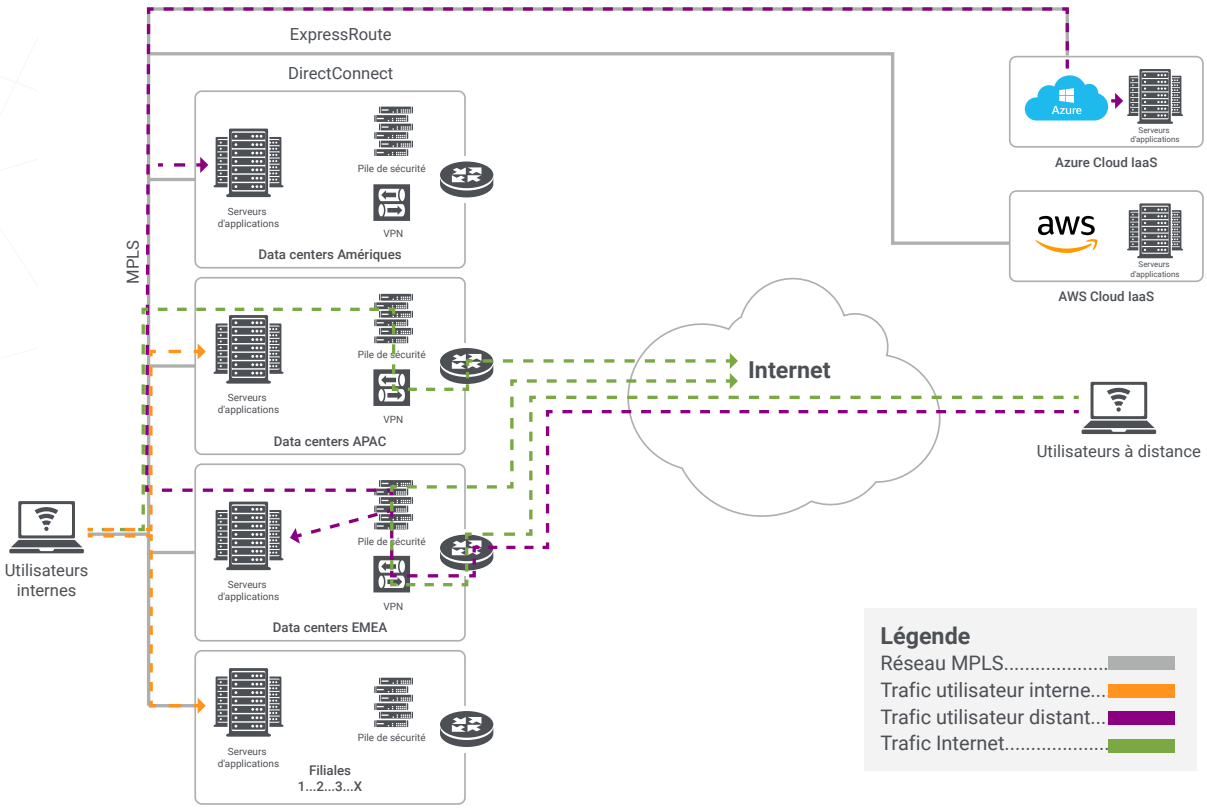
- Différences architecturales entre les technologies d'accès existantes et le ZTNA
- Présentation d'une architecture de référence pour le déploiement de ZTNA
- Trois phases à respecter lors de l'adoption de ZTNA au sein de votre entreprise
- Conseils et recommandations pour tirer le meilleur parti de votre déploiement ZTNA

Avant de commencer, prenez le temps de lire « Atténuer les risques grâce au périmètre défini par logiciel ». Ce blog fournit une présentation initiale des services d'accès réseau Zero Trust.

À présent, examinons l'architecture ZTNA en tant que moyen de connecter les utilisateurs autorisés à des applications privées spécifiques, sans jamais les placer sur le réseau.

Où en êtes-vous aujourd'hui ? Un regard sur le VPN au sein de l'entreprise.

L'architecture que nous retrouvons dans de nombreuses entreprises peut être décrite dans ce diagramme général. Oui, je sais que le nombre et l'emplacement des data centers, des routeurs, des pare-feu, des concentrateurs VPN et du réseau MPLS ne seront pas strictement conformes au diagramme, mais je pense qu'il fournit une représentation suffisamment proche des composants. Les entreprises ont déployé de nombreux autres dispositifs de réseau et de sécurité, notamment des proxy en ligne, des espaces Sandbox, des pare-feu L7, des solutions AV et DLP, etc. Par souci de simplicité, j'ai regroupé l'ensemble du concept de sécurité lié à Internet sous le nom de Security Stack (Pile de sécurité) dans les diagrammes.



J'aimerais souligner quelques points à propos de ce type d'architecture traditionnelle :

01 Les utilisateurs distants se connectent via un VPN à l'un des data centers et sont placés sur le réseau de l'entreprise. D'après mon expérience auprès de nombreuses entreprises, le réseau est relativement plat, les ACL sont plutôt limitées, exposant ainsi toute l'infrastructure et les réseaux du data center de l'entreprise à chaque utilisateur distant.

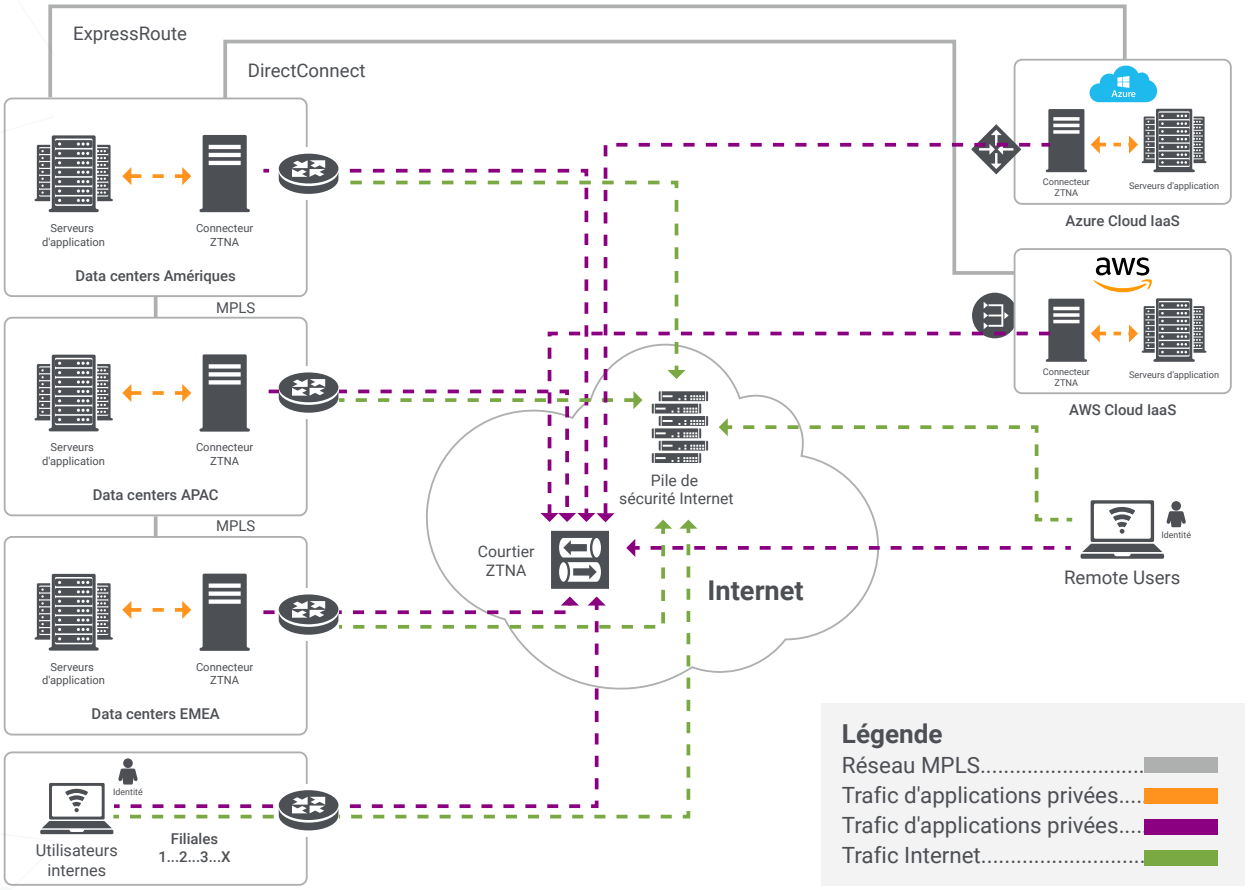
02 Tout le trafic Internet des utilisateurs distants sera acheminé vers le data center pour y être inspecté à l'aide de la pile de sécurité (matérielle) de l'entreprise. C'est ce qu'on appelle un tunnel VPN complet. Il s'agit du moyen idéal pour les équipes de sécurité qui doivent garantir la sécurité des utilisateurs lorsqu'ils ne sont pas sur le réseau de l'entreprise, mais qui peut avoir un impact négatif sur l'expérience utilisateur lorsque toutes les applications Internet/SaaS sont soumises à un backhauling au lieu d'une sortie locale. De nombreux utilisateurs disposent aujourd'hui de connexions Internet haut débit à domicile qui sont plus rapides que certains canaux WAN d'entreprise. Même dans le Tennessee quelque peu rural où j'habite, je dispose d'une connexion en fibre optique de 1 Gbit/s via mon FAI !

03 Les utilisateurs internes sont généralement sur des réseaux d'appareils/utilisateurs, qu'ils soient physiques ou sans fil, mais ils sont toujours en mesure d'acheminer/connecter leur trafic vers tous les réseaux du data center puisque ces réseaux sont traditionnellement « fiables ». L'accès aux applications internes passe par le LAN, et les applications Internet/SaaS passent par la pile de sécurité avant de sortir vers le FAI. Le problème est illustré par ce postulat erroné : étant donné que vous « possédez » et contrôlez le réseau, vous devriez automatiquement faire confiance à tous les utilisateurs et appareils qui s'y trouvent.

Notez les points suivants : l'accès entrant est requis depuis Internet (VPN) pour l'accès à distance ; en outre, les utilisateurs internes peuvent communiquer directement avec tous les serveurs d'application, quelle que soit leur identité.

Architecture de référence facilitant l'accès aux applications internes sans augmenter les risques

L'objectif final d'une architecture définie par logiciel est de dissocier l'accès aux applications de l'accès au réseau. Il n'est plus nécessaire de placer les utilisateurs sur le réseau, les applications privées ne sont accessibles qu'aux utilisateurs autorisés, les adresses IP ne sont jamais exposées sur Internet et la complexité de la gestion des segments de réseau, des politiques de pare-feu et des ACL est supprimée. Le diagramme suivant présente un aperçu simplifié du résultat final.



Avec cette nouvelle architecture définie par logiciel, vous remarquerez qu'il existe une séparation claire entre les réseaux du data center/d'application, les utilisateurs distants et les utilisateurs internes. Peu importe que votre entreprise possède seulement deux data centers basés aux États-Unis, une dizaine de data centers mondiaux, quelques environnements Azure/AWS/GCP, etc… Les résultats parlent d'eux-mêmes :

01 Un réseau privé, tel que MPLS ou même des VPN site à site, ne devrait être nécessaire qu'entre les data centers et les environnements IaaS cloud où une communication de serveur à serveur est requise. Si votre entreprise a déplacé le niveau Web du site « www » vers AWS mais que la base de données SQL backend se trouve toujours dans un data center physique, vous aurez toujours besoin d'une connectivité privée (faible latence, large bande passante) entre ces sites.

02 L'accès à distance ne nécessite plus de connectivité entrante pour les utilisateurs, comme par exemple vpn.société.com. Cette architecture place le plan d'orchestration (contrôle) dans le cloud où la communication des utilisateurs est interrompue. Les passerelles, connues dans le monde Zscaler sous le nom de ZPA App Connectors, n'ont pas besoin de ports d'écoute entrants, un enregistrement IP/DNS public. Ces connecteurs communiquent en sortie via TLS vers le plan d'orchestration basé sur un SaaS. Les applications internes ne sont ouvertes que lorsque l'identité d'un utilisateur a été vérifiée et comparée aux politiques d'accès.

- Si un utilisateur est autorisé à accéder à une application/ressource interne, le plan d'orchestration assemble les connexions TLS sortantes entre les connecteurs et les appareils des utilisateurs. Cependant, cet utilisateur n'est pas placé sur le réseau. Les applications basées sur le DNS sont donc obscurcies, ce qui signifie que les véritables adresses IP privées des serveurs d'applications ne sont pas exposées aux appareils des utilisateurs. En revanche, une adresse IP artificielle est créée dynamiquement sur le client pour chaque application à laquelle il accède.

- Si un utilisateur n'est pas autorisé à accéder à une application interne, aucun trafic réseau généré n'entrera jamais dans le data center. La demande sera bloquée dans le cloud, ce qui élimine le risque de laisser les utilisateurs atteindre la « porte d'entrée » des serveurs d'applications critiques. La meilleure manière d'expliquer cela est de bloquer les utilisateurs au niveau du cloud avant qu'ils ne puissent établir une session SSH ou RDP sur un serveur. Bien que l'utilisateur ne soit probablement pas en mesure d'authentifier la session SSH/RDP (en dehors de la force brute ou avec des informations d'identification volées), cette architecture élimine ce risque. Le plus beau dans tout ça ? Chacune de ces tentatives est enregistrée, ce qui permet à votre équipe de sécurité de surveiller de manière proactive (et réactive) ce que les utilisateurs sont en train de faire. Un exemple serait d'envoyer tous les journaux à votre SIEM, tel que Splunk, et de créer une alerte si un utilisateur génère un nombre X de politiques bloquées en un nombre X de minutes sur les mêmes serveurs/ports ; par exemple, en essayant de se connecter en SSH à sap.société.com 20 fois en 5 minutes. Si l'utilisateur est bloqué par le biais d'une politique, vous êtes en sécurité et vous pouvez intervenir de manière proactive afin de vérifier si l'appareil de l'utilisateur est compromis ou si l'utilisateur avait des intentions malveillantes. Si l'utilisateur n'avait pas été bloqué par une politique, les sessions SSH auraient été ouvertes mais le serveur aurait rejeté des informations d'identification incorrectes, ce qui signifie que l'utilisateur aurait été autorisé, mais aurait oublié le mot de passe administrateur (root) !

03 Les réseaux des utilisateurs doivent tous être traités comme des cybercafés ou des réseaux WiFi invités. Que l'utilisateur soit sur le site principal au siège social, dans une filiale, dans une usine de fabrication ou simplement en déplacement, il n'y a aucune raison de placer l'utilisateur sur le réseau où il peut accéder à vos serveurs d'applications et vos data centers. Il est important de noter que certaines filiales peuvent avoir des exigences autres que l'accès de l'utilisateur à l'application. Dans un tel cas, les appareils IoT et les communications de type serveur à serveur auraient quand même besoin d'une connectivité réseau privée. Cependant, même si une telle exigence existe, il est préférable de séparer ces réseaux de ceux des utilisateurs.

04 L'accès à Internet, alias la pile de sécurité, doit également être modernisé pour permettre une sécurité et une expérience utilisateur optimales. Lorsque vous dissociez les utilisateurs du réseau, vous devriez envisager d'envoyer le trafic Internet directement des utilisateurs plutôt que vers un data center centralisé pour inspection. Pour les filiales, cela peut se résumer à utiliser un routeur, un pare-feu ou un dispositif SD-WAN existant pour diriger tout le trafic Internet vers une solution de sécurité cloud, telle que la plateforme Zscaler Internet Access. La pile de sécurité complète est offerte en tant que service, et avec plus de 100 sites mondiaux, cela signifie que vous pouvez envoyer tous les sites de l'entreprise aux sites Zscaler les plus proches pour inspection. Même si l'utilisateur est en déplacement, le client unifié Zscaler App, un agent de transfert léger déployé sur les appareils mobiles et les ordinateurs portables de l'utilisateur, peut fournir l'expérience utilisateur nécessaire (en envoyant le trafic Internet localement au nœud Zscaler le plus proche au lieu du backhauling), tout en procurant à l'équipe informatique les contrôles de sécurité et la visibilité nécessaires.

Trois phases permettant l'adoption d'une architecture ZTNA

Les architectes demandent souvent « quelle est la meilleure façon de commencer ? ». L'une de mes réponses préférées est « ça dépend ». Je sais que de nombreux ingénieurs et architectes peuvent se reconnaître dans cette réponse, car un grand nombre de résultats peuvent être atteints en fonction des besoins, des exigences et d'une configuration spécifiques. Cependant, il est de notre responsabilité de fournir aux entreprises les recommandations de bonnes pratiques pour les accompagner dans leur parcours. Je tiens à préciser que l'approche progressive discutée dans cette section n'est pas un ensemble concret d'étapes que chaque entreprise doit suivre. Il s'agit d'une approche de haut niveau que nous avons observée dans de nombreux scénarios pour répondre aux exigences actuelles, tout en permettant à l'entreprise d'adopter le concept de réseau Zero Trust. La confiance n'est jamais implicite et l'accès est adaptatif, basé sur des politiques contextuelles définies par les administrateurs : utilisateur, appareil, service, etc.

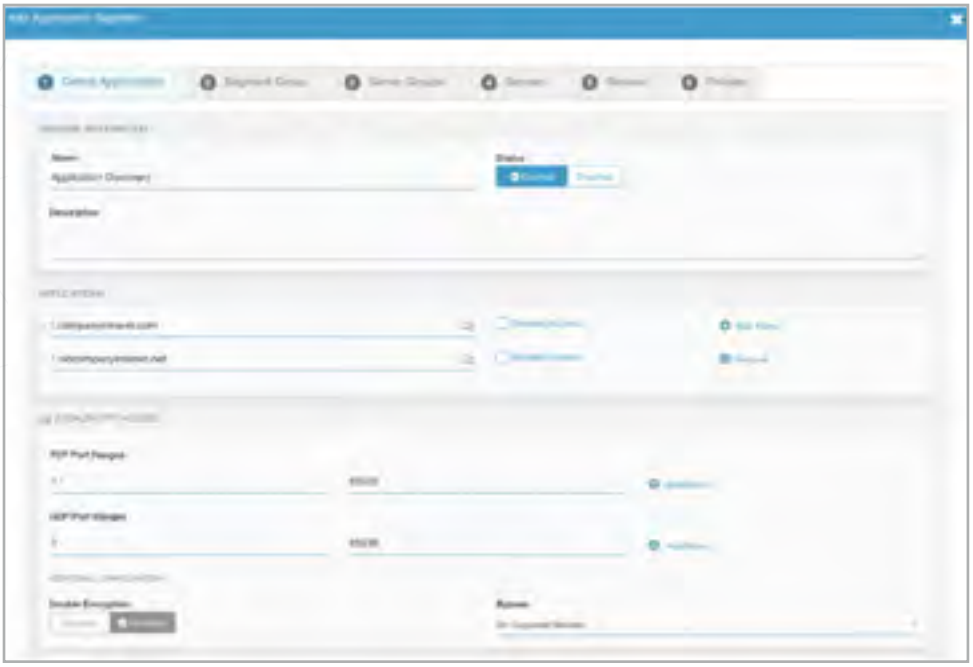
L'approche ressemble presque à un parcours à petits pas : commencez par les utilisateurs distants, développez des segments, puis tirez parti du ZTNA pour l'accès aux applications privées pour tous les utilisateurs, indépendamment de leur emplacement. Vous devrez tenir compte de la manière dont les utilisateurs accèdent aux applications et aux services, de la répartition (quantités et types) de vos sites (data centers, environnements cloud IaaS et sites physiques à partir desquels les employés travaillent) et des échéances liées à un projet. Dans de nombreux cas, un renouvellement du VPN pourrait servir de catalyseur pour adopter ZTNA plutôt que d'acheter un VPN de nouvelle génération ou « toujours actif » qui apporte les mêmes problèmes que votre VPN actuel.

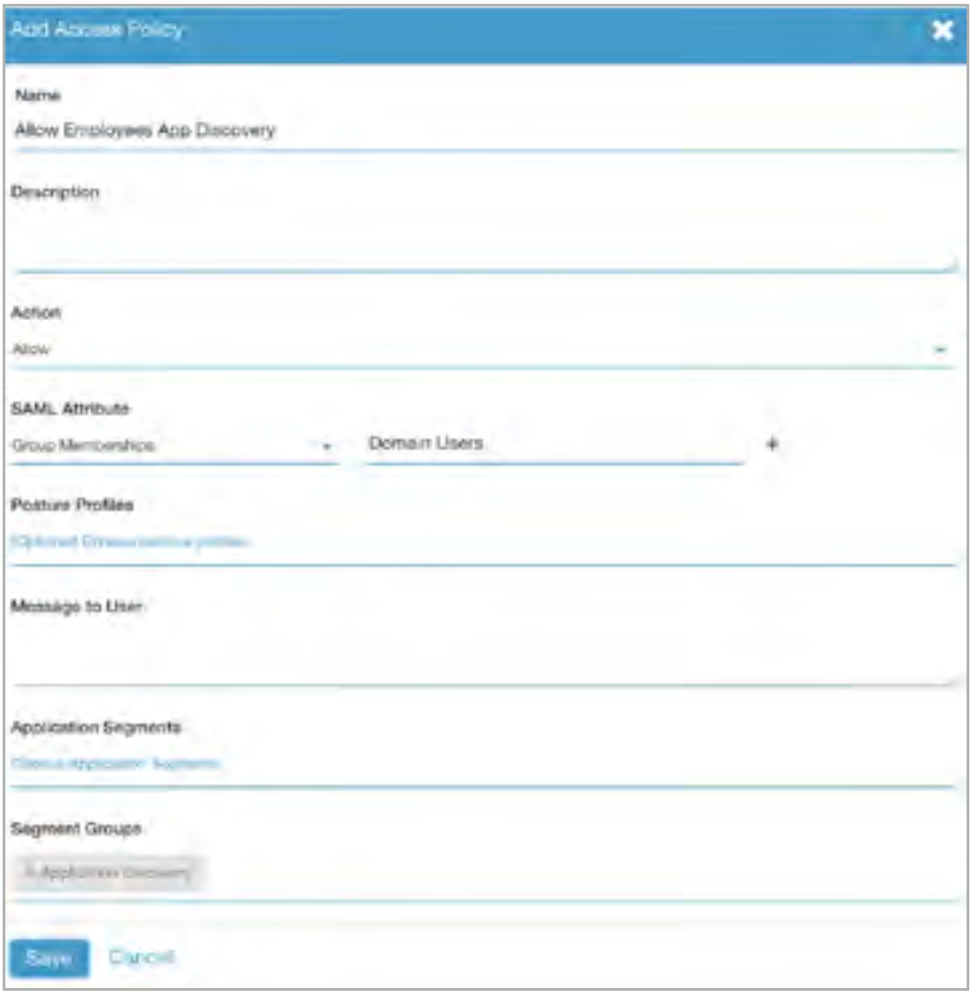
Phase 1 Déployer le ZTNA pour l'accès à distance et la découverte d'applications

Dans cette phase, vous commencerez par remplacer la solution VPN d'accès à distance existante. Pour ce faire, vous devrez peut-être déployer ZTNA avec des niveaux d'accès similaires à ceux de votre VPN d'accès à distance actuel. Ceci est essentiel car vous devez vous assurer que votre nouvelle initiative n'est pas perçue comme un obstacle à la productivité des utilisateurs distants.

Vous devrez également savoir quelles applications privées sont exécutées dans votre environnement afin de réduire votre surface d'attaque et d'éliminer l'informatique fantôme. Il y a de fortes chances qu'il y ait beaucoup plus d'applications que vous ne le pensez. Notre solution appelée Zscaler Private Access (ZPA) résout ce problème grâce à notre fonction de découverte des applications. Il est impossible d'avoir connaissance de toutes les applications/services internes auxquels chaque utilisateur doit accéder. C'est pourquoi la fonction de découverte d'applications vous permet en bref d'utiliser des caractères génériques, tels que *.société.com, *.société.net, tous les ports TCP et UDP.

Une fois qu'un utilisateur s'est abonné au service, le client détecte automatiquement le moment où l'utilisateur n'est plus sur le réseau de l'entreprise ; toutes les applications internes transitent désormais par ZTNA lorsque l'utilisateur est hors réseau. Il n'est plus nécessaire de lancer un client VPN et l'utilisateur peut accéder aux ressources internes comme auparavant. Tous ces journaux d'accès sont disponibles dans la console d'administration ZPA et peuvent également être transmis en quasi temps réel au SIEM de votre choix, ce qui permet une visibilité granulaire sur les applications auxquelles les utilisateurs accèdent.



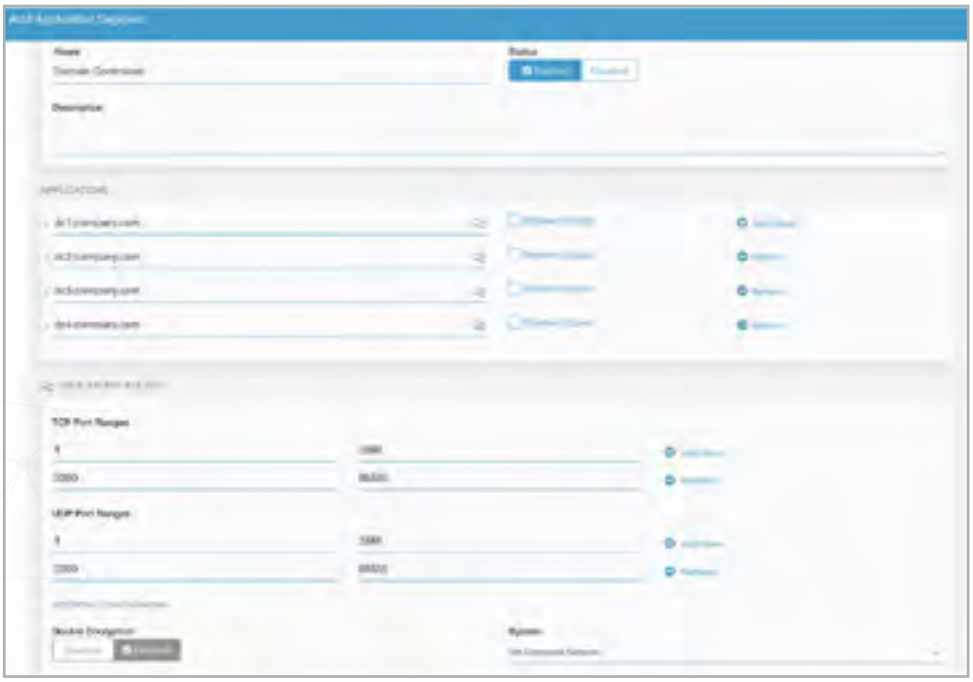


Comme le réseau privé interne (MPLS, VPN site à site) existe très probablement encore, le client Zscaler App désactivera automatiquement ZPA lorsque l'utilisateur reviendra au réseau d'entreprise. Désormais, tous les accès aux applications internes se font sur le réseau local sans Zscaler sur le trajet.

Phase 2 Exploiter la micro-segmentation pour assurer une connectivité basé sur le moindre privilège

Dans cette phase, vous devrez définir des politiques qui séparent les applications privées en segments, et fournir un accès à ces segments via les attributs d'identité de l'utilisateur.

Comme les grandes entreprises peuvent compter des centaines ou des milliers d'applications/services uniques, beaucoup d'entre elles ont tendance à commencer par segmenter les ports de gestion, tels que TCP 22 (SSH) et TCP/UDP 3389 (RDP), et ne fournissent un accès à ces ports qu'aux utilisateurs informatiques. Naturellement, des besoins ponctuels peuvent toujours exister, mais cette segmentation peut contribuer à réduire la surface des utilisateurs qui se connectent à des serveurs auxquels ils ne devraient même pas pouvoir accéder. Par exemple, vos commerciaux ne devraient probablement pas pouvoir accéder au port TCP 3389 sur un serveur Windows qui héberge votre application SAP ; ils ne devraient pouvoir accéder qu'à la partie Windows Web frontale, qui se trouve sur les mêmes serveurs, mais sur les ports TCP 80/443.



Dans l'idéal, il s'agit de serveurs d'infrastructure qui peuvent être des contrôleurs de domaine/services, des clients de logiciels de sécurité, des clients de déploiement de logiciels, etc. : ceux-ci peuvent être facilement segmentés car les hôtes sont bien connus.

La segmentation des applications est un processus continu, la recommandation générale étant de donner la priorité aux applications les plus critiques pour l'entreprise et qui ne doivent être accessibles que par des types d'utilisateurs connus.

À mesure que vous segmentez les applications, celles-ci sont retirées du « pool » de découverte des applications. Cela signifie que vous pouvez les mélanger pour vous assurer que les utilisateurs peuvent toujours accéder aux applications de vos domaines que vous n'avez pas explicitement définies, mais qu'ils peuvent également accéder aux applications connues sur les ports de service requis.

REMARQUE : N'oubliez pas non plus la sécurité Internet.

Bien que nous nous intéressions aux applications privées dans ce guide, il est tout aussi essentiel de fournir une pile de sécurité pour tout le trafic Internet. De nombreuses entreprises envisagent une pile de sécurité entrante et sortante plus moderne, entièrement basée sur le cloud, au lieu de s'appuyer sur des appliances ou des appliances virtuelles (c'est-à-dire des pare-feu). Chez Zscaler, notre solution de sécurité du trafic cloud sortant s'appelle Zscaler Internet Access (ZIA).

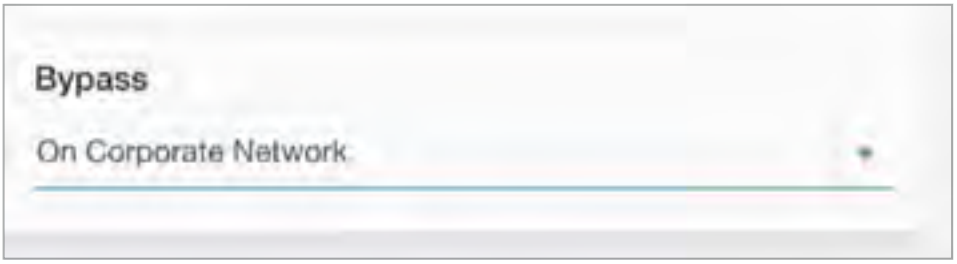
Phase 3 ZTNA pour l'accès aux applications privées de tous les utilisateurs (pas uniquement les utilisateurs distants)

Vous êtes maintenant prêt pour la dernière phase. Désormais, tous les accès aux applications privées seront basés, par défaut, sur des paramètres précis qui permettent une connectivité explicite et basée sur le moindre privilège uniquement.

ZPA fournit cette connectivité de l'intérieur vers l'extérieur via des micro-tunnels TLS doublement chiffrés qui sont générés pour chaque session et créent un segment sécurisé entre un utilisateur autorisé et une application privée spécifique.

Vous vous souvenez peut-être que j'ai mentionné plus tôt le fait que Zscaler App peut détecter le réseau d'entreprise. Cela signifie que dans ZPA, chaque segment d'application dispose d'une option de configuration pour 1) contourner ZPA lorsqu'il se trouve sur le réseau d'entreprise, 2) toujours contourner ZPA, ou 3) ne jamais contourner ZPA. Dans la phase 1, vous avez déployé des segments d'application en utilisant l'option 1, mais qu'en est-il de l'accès sécurisé non seulement des utilisateurs distants, mais de tous les utilisateurs ? Pour cela, il vous suffit de changer les segments d'applications pour qu'ils ne contournent jamais ZPA. Ainsi, même lorsque les utilisateurs se trouvent dans un bureau physique, tous les accès aux ressources internes passent par cette solution d'architecture de confiance explicite, et ne sont jamais simplement acheminés sur le réseau local directement vers les serveurs d'application dans votre data center !

Passer de



à

Un vrai jeu d'enfant, non ? Je pense que les défis liés à ce changement demeurent en dehors de notre plateforme elle-même. Comme vous vous en souvenez peut-être, l'objectif final est généralement de supprimer complètement les réseaux du serveur d'applications/data center de tous les réseaux utilisateur. Cela signifie qu'il n'y a pas de connectivité entre les filiales, les usines de fabrication, etc. (c'est-à-dire, il n'y a pas de connectivité entre les réseaux UTILISATEUR de ces sites) et le data center.

Dernières considérations et conseils professionnels :

Le plus simple est peut-être de commencer par un nouveau bureau de petite taille qui n'est pas encore sur le réseau. Ouvrez ce bureau avec une simple connexion Internet haut débit. Faites passer tout le trafic lié à Internet par une plateforme de sécurité cloud (telle que ZIA) et faites passer tout le trafic des applications privées par la plateforme ZPA.

Traitez le nouveau bureau comme si vous ouvriez un cybercafé ! Encore une fois, gardez à l'esprit que nous sommes aujourd'hui en mesure de fournir cette connectivité pour les utilisateurs vers les applications ; certains emplacements, tels qu'une usine de fabrication avec des capteurs, des dispositifs IoT et des serveurs, auront probablement encore besoin de communiquer avec vos data centers par le biais d'un MPLS ou d'un VPN privés. Traitez ces réseaux de sites comme des data centers et éloignez simplement les utilisateurs de ces derniers ; tous les utilisateurs utiliseront la connexion « WiFi invité » et l'accès aux applications internes sera négocié avec les utilisateurs autorisés.

En fin de compte, il existe une grande effervescence et un fort battage autour des architectures ZTNA, mais le véritable objectif est d'offrir l'expérience que les utilisateurs souhaitent, avec la sécurité nécessaire dans le cadre d'applications privées. Il faudra du temps à votre entreprise pour adopter cette nouvelle méthode, mais vous, en tant qu'architecte réseau, pouvez poser les bases (plateformes) qui la rendront possible.

Vous pouvez faire l'expérience de ZPA par vous-même en vous inscrivant à un essai hébergé de 7 jours sur **https://www.zscaler.fr/zpa-interactive.**

Zscaler, Inc.
110 Rose Way Orchard
San José, Californie
+1 408 533 0288
www.zscaler.fr