FICHE TECHNIQUE

Sécuriser les Communications des Charges de Travail avec Cloud Connector

Accès simple et sécurisé des charges de travail à l'internet et aux applications privées avec une architecture direct-to-cloud.

Faire évoluer les communications réseau pour le cloud

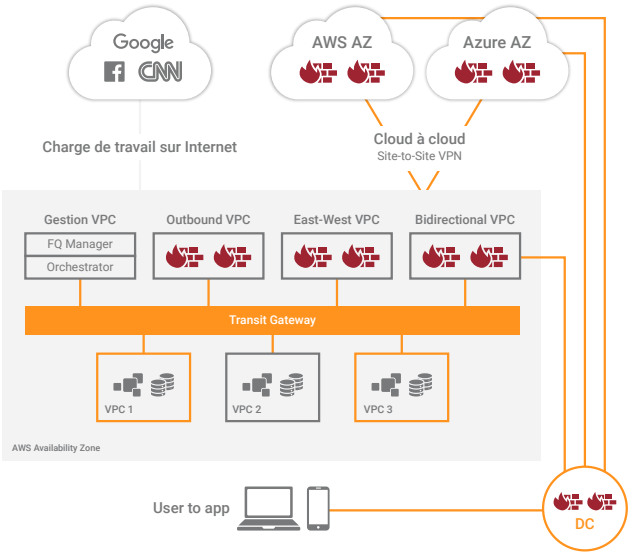
À mesure que les charges de travail migrent vers le cloud et que les utilisateurs deviennent de plus en plus mobiles, les entreprises ont un besoin urgent et impérieux de transformer leurs réseaux pour assurer la compétitivité de l'entreprise. Il n'est plus possible d'étendre les réseaux existants et d'appliquer une sécurité basée sur le périmètre à l'aide de pare-feux. Pour les entreprises qui modernisent leur infrastructure, assurer une communication efficace de la charge de travail est devenu une exigence incontournable. Cloud Connector de Zscaler a complètement réinventé les communications de charge de travail pour fournir un accès simple et sécurisé aux charges de travail sur Internet et aux applications privées. Contrairement à la sécurité des réseaux traditionnels, Cloud Connector utilise une architecture directe au cloud, qui s'appuie sur la plateforme éprouvée Zero Trust Exchange de Zscaler. L'adoption de Cloud Connector pour transformer leurs réseaux entraine de nombreux avantages pour les clients, notamment une meilleure sécurité, des opérations plus simples, une visibilité accrue, une meilleure disponibilité, des performances améliorées et des coûts réduits.

Défis de connectivité des charges de travail avec la sécurité réseau traditionnelle

Lorsque les entreprises tentent de connecter des charges de travail à Internet ou à d'autres applications dans des environnements de clouds publics ou de data center, elles se trouvent confrontées à un certain nombre de défis en utilisant d'anciennes architectures réseau et de sécurité, notamment :

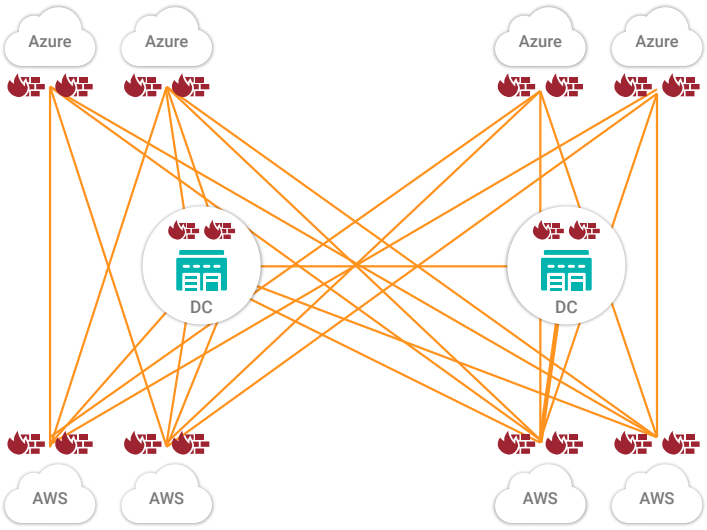
- Le **risque accru de menaces latérales et d'attaques basées sur Internet** du fait de l'utilisation de solutions de connectivité traditionnelles centrées sur le réseau, telles que les VPN cloud, les VPN site à site, les pare-feux ou les technologies WAN, qui étendent de manière anormale le réseau de confiance d'un client sur Internet à d'autres clouds et environnements sur site, augmentant ainsi la surface d'attaque du réseau. Un travail d'assemblage d'appliances de sécurité, d'outils et de politiques non standard augmente les risques de sécurité en raison des lacunes dans la couverture de sécurité, qu'elles soient connues ou non.
- Une **complexité croissante** en raison d'un filtrage compliqué des itinéraires, de multiples sauts de réseau, d'appliances virtuelles pour la mise en réseau et la sécurité, et d'une gestion fragmentée des politiques pour l'introduction de ces anciens modèles dans le cloud. Gérer cette complexité est une tâche difficile pour les équipes de sécurité, car elles ont du mal à appliquer une connectivité normalisée des charges de travail et des politiques de sécurité dans les environnements hybride et multicloud.
- Le **manque de visibilité** sur les voies de connectivité des applications crée des angles morts au niveau du réseau et de la sécurité. Les charges de travail du cloud sont devenues plus distribuées et les environnements ont évolué. La connexion de ces charges de travail distribuées nécessite des réseaux obscurs à sauts multiples et une connexion en série avec plusieurs appliances de réseau et de sécurité. Cette connectivité complexe et l'absence de journalisation centralisée font que les opérateurs ne maîtrisent rien aux communications d'applications.
- Des **performances et une évolutivité médiocres** en raison du nombre croissant de services de réseau et de sécurité dans les environnements de cloud public, le hairpinning du trafic et les points d'étranglement pour le contrôle et l'inspection centralisés de la sécurité.
- Des **coûts exorbitants** dus aux appliances de sécurité réseau obsolètes (par exemple, pare-feux, IPS, routeurs et autres produits ponctuels), au surdimensionnement des services réseau pour compenser le manque d'évolutivité et à l'utilisation accrue de services natifs du cloud tels que le peering de transit.

Traditionnel : étendre le WAN d'entreprise au cloud



Exorbitant, complexité opérationnelle, expérience utilisateur médiocre, piètre sécurité en raison de mouvements latéraux sur le WAN

Pour le multi-cloud, la complexité et le risque sont multipliés



Un maillage de VPN site à site (personnel, partenaires, appareils, clients)
Accroissement de la surface d'attaque et du risque de déplacement latéral des menaces

Corporate network Public Internet Corporate network

Cloud Connector introduit l'accès Zero Trust aux charges de travail du cloud

Cloud Connector fournit aux charges de travail un accès rapide et fiable à Internet et aux applications privées grâce à une architecture directe au cloud, qui offre une sécurité élevée et une simplicité opérationnelle. Cloud Connector élimine la surface d'attaque réseau en connectant directement les charges de travail à Internet et aux applications privées à l'aide d'une architecture proxy complète. En outre, cette architecture simplifie considérablement les communications de la charge de travail en éliminant le routage, les VPN, les passerelles de transit, les hubs de transit et les pare-feux, tout en permettant un transfert flexible et en facilitant la gestion des politiques grâce à l'utilisation du cadre éprouvé des politiques ZIA et ZPA.

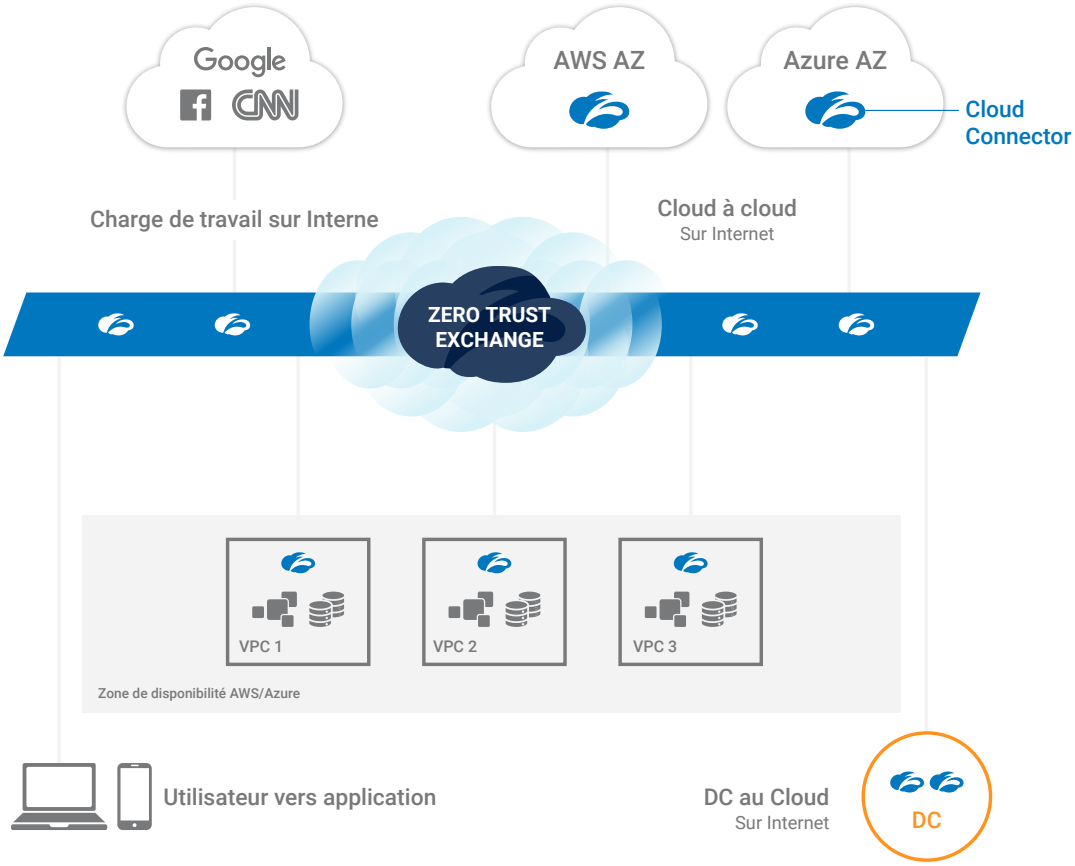
Ce n'est qu'en utilisant Zero Trust Exchange que l'architecture directe au cloud est rendue possible. Cloud Connector transfère directement toutes les communications de charge de travail vers Zero Trust Exchange, où les politiques ZIA ou ZPA peuvent être appliquées pour une inspection de sécurité complète et un contrôle des communications de charge de travail basé sur l'identité. De Zero Trust Exchange, les communications sont ensuite transférées vers n'importe quelle destination, qu'il s'agisse d'Internet ou d'autres applications privées dans un cloud public ou un data center sur site. Cette approche unique offre trois avantages majeurs :

- Abandon de la connectivité VPN basée sur le réseau au profit d'une communication basée sur l'identité et les applications pour une réelle sécurité Zero Trust
- Élimine l'ancienne architecture cloisonnée sans compromettre la sécurité ; pas besoin des traditionnels produits tels que les proxys Squid, les passerelles NAT, les IPS, etc.
- Connectivité distribuée et évolutive partout où elle est nécessaire, mais centralisation et automatisation de la gestion des politiques pour simplifier les communications des charges de travail

Le Cloud Connector est bien ajusté pour aider une entreprise à répondre à ses priorités de transformation du réseau de nombreuses façons. Il étend la connectivité de la charge de travail vers la charge de travail, à l'aide de principes Zero Trust, sur des réseaux disjoints et de multiples clouds, notamment les régions AWS, Microsoft Azure, Google Cloud ainsi que des data center sur site. Cloud Connector fournit également un accès Internet sécurisé pour les charges de travail dans les cloud publics et les data center. Et toutes ces capacités sont fournies via une instance de politique unifiée pour le transfert de trafic, la sécurité et l'accès Zero Trust à travers ces environnements hétérogènes.

Tirer parti du Zero Trust pour les multi-clouds

N'étendez pas votre WAN sur plusieurs clouds.
Connectez les régions DC, Azure, AWS et GCP par Internet



Réduction des coûts et de la complexité, expérience utilisateur exceptionnelle.
Une meilleure sécurité grâce au modèle Zero Trust

Avantages de Cloud Connector

Déploiement plus simple, sans configurations réseau compliquées. Les approches traditionnelles nécessitent des configurations de routage complexes via des passerelles de transit, des hubs de transit et des SNAT, qui doivent être répétées pour chaque VPC et dans chaque cloud. En revanche, Cloud Connector n'a besoin que d'un chemin par défaut vers Internet. La gestion des politiques de transfert de trafic et de sécurité est centralisée et normalisée dans Zero Trust Exchange, quelle que soit la source ou la destination des communications de la charge de travail.

Visibilité totale, de bout en bout, avec une connectivité directe au cloud. L'ancienne méthode repose sur une mise en réseau obscure à sauts multiples, qui rend très difficile la maîtrise du flux de trafic. Qui plus est, la journalisation est dispersée à travers divers produits réseau. Cloud Connector se connectant directement au cloud, les opérateurs bénéficient d'une visibilité et d'un contrôle exhaustifs sur la façon dont les charges de travail communiquent. La journalisation est centralisée et diffusée en temps réel. Les journaux peuvent être exportés vers un SIEM ou une solution de surveillance de votre choix pour corrélation et analyse.

Hyper évolutivité, sans points d'étranglements centralisés. Les architectures traditionnelles exigent que tout le trafic soit canalisé vers une infrastructure centralisée, impliquant des passerelles de transit, des hubs et des pare-feux virtuels qui ne disposent ni de l'élasticité ni de l'évolutivité nécessaires pour gérer les pics de débits. L'architecture moderne Zero Trust Exchange opère à grande échelle dans plus de 150 data centers à travers le monde et gère toute augmentation des communications avec une évolutivité élastique et horizontale.

Haute disponibilité sans réplication inutile des services. Les approches existantes nécessitent une architecture de disponibilité complexe de plusieurs pare-feux et configurations de mise en réseau qui doivent être répliquées sur plusieurs zones, régions et clouds. L'architecture directe au cloud de Cloud Connector simplifie considérablement les exigences de configuration cloud, car tous les services requis sont fournis de manière transparente dans Zero Trust Exchange, à grande échelle. Sur le site du client, le basculement automatique avec redondance N+2 est fourni pour le transfert et la sécurité.

Coûts réduits grâce aux services rationalisés fournis par Zero Trust Exchange. Les clients n'ont plus à fournir des niveaux de services excessifs et à payer pour les durées d'inactivité des pare-feux, des hubs de transit et des passerelles NAT, répliqués dans chaque environnement cloud, qui augmentent rapidement. Avec Cloud Connector, il n'y a pas de coûts injustifiés et les clients ne sont facturés que des services de sécurité consommés et non la mise en réseau ou l'accès. Pas besoin de payer pour des pare-feux ou des proxys virtuels dans les environnements des clients.

Valeur ajoutée de Cloud Connector

Cloud Connector repose sur Zero Trust Exchange de Zscaler, qui connecte en toute sécurité les utilisateurs, les appareils et les applications à l'aide de politiques d'entreprise sur n'importe quel réseau et sur n'importe quel cloud, à grande échelle.

- Les charges de travail des applications sont directement connectées les unes aux autres, indépendamment du réseau d'entreprise sous-jacent, du VPN ou du WAN.
- Les applications sont invisibles pour le monde extérieur et ne présentent aucune surface d'attaque.
- Architecture proxy multi-entité spécialement conçue pour maintenir, inspecter et appliquer la politique.
- L'inspection de haute performance s'effectue par une architecture multi-accès et d'analyse unique conçue pour évoluer.
- Gestion fine des politiques de transfert pour le trafic Internet et non-Internet, à l'aide des politiques de Zscaler Internet Access ou de Zscaler Private Access.
- Politiques unifiées et standardisées pour AWS, Azure, Google Cloud et les data center sur site. Cela inclut la gestion de la politique, le surveillance du trafic, les journaux de suivi.

Cas d'utilisation de Cloud Connector

Transformation digitale

Au fur et à mesure que les entreprises migrent leurs applications vers le cloud et créent des applications natives du cloud, les modèles de mise en réseau et de sécurité sur site perdent du terrain. La transformation digitale nécessite une transformation réseau, qui s'appuie sur un nouveau modèle de communication des charges de travail ; un modèle dans lequel les charges de travail communiquent en toute sécurité avec n'importe quelle destination et indépendante du réseau sous-jacent. Cloud Connector est spécialement conçu pour permettre la transformation digitale.

Connectivité de la charge de travail sans VPN

Les entreprises peuvent désormais connecter directement les charges de travail aux applications privées sans étendre leur WAN ni compter sur des VPN, lesquels augmentent la surface d'attaque du réseau.

La mission de Zero Trust

Zero trust part du principe que le réseau a été compromis et ne peut plus être fiable. Avec cette donne, Cloud Connector connecte directement les charges de travail à Internet ou aux applications privées sans connecter les réseaux. Chaque connexion est contrôlée et enregistrée à des fins d'audit.

Sécurisation de l'accès à Internet pour les charges de travail cloud.

Les charges de travail peuvent être considérées comme le reflet des utilisateurs. Tout comme les utilisateurs, les charges de travail peuvent être directement connectées au cloud via Zscaler Internet Access et bénéficier d'un cadre de politique et d'une inspection de sécurité identiques ainsi que du même contrôle d'accès. Les pare-feux virtuels ne sont pas nécessaires.

Fusions et acquisitions

La fusion de deux réseaux disparates est un véritable défi et prend énormément de temps. Les problèmes vont des chevauchements d'adresses IP aux difficultés de routage, en passant par le risque accru de sécurité dû à l'extension de la surface d'attaque du réseau lorsque deux réseaux sont combinés. Avec Cloud Connector, il n'est pas nécessaire de fusionner les réseaux. Ils peuvent être séparés et les charges de travail d'un environnement peuvent, avec une extrême précision, se connecter aux applications privées dans un autre environnement, rapidement et sans interruption.

Connectivité des filiales

La connexion d'applications de filiales aux applications privées ou à Internet est devenue beaucoup plus facile grâce à Branch Connector, qui est une version sur site de Cloud Connector. Branch Connector complète les SD-WAN et les partenaires Zscaler avec tous les principaux fournisseurs SD-WAN.

Fiche technique des fonctionnalités

Approvisionnement sans aucune interaction et déploiement automatisé

- Approvisionnement sans aucune interaction avec des modèles définis par le système pour AWS et Azure
- Déploiement entièrement automatisé (AWS CloudFormation, Modèles Azure Resource Manager et Terraform)
- Découverte dynamique des zones géographiques de clients, zones de disponibilité, VPC/VNET
- Surveillance SLA et basculement intégrés
- Disponible sur les marketplaces AWS et Azure

Politique de transfert granulaire pour le trafic Internet et non-Internet

- Options pour envoyer le trafic vers ZIA, ZPA ou Direct (en contournant les services Zscaler)
- Critères flexibles de sélection du trafic : emplacement, sous-emplacement, groupe d'emplacements, 5-tuple ou FQDN
- Disponibilité intégrée avec basculement transparent vers le prochain service pop disponible

Politique unifiée pour le transfert et la sécurité grâce à Cloud Connector et ZIA

- Les emplacements sont créés de manière dynamique pour les VPC/VNET
- Les emplacements dynamiques de connecteurs cloud sont synchronisés dans la plateforme ZIA
- Les emplacements créés par les connecteurs cloud sont comme tout autre emplacement ZIA existant. Toutes les politiques de sécurité peuvent être activées, notamment les IPS, le proxy SSL, le filtrage d'URL, la protection des données

Politique Zero Trust unifiée pour les utilisateurs vers les serveurs et les serveurs vers les serveurs

- ZPA fournit une politique unifiée pour l'utilisateur vers l'application et le serveur vers le serveur
- La politique ZPA existante est améliorée pour inclure un nouveau type de client (Cloud Connector) afin de prendre en charge la connectivité entre serveurs
- Les groupes Cloud Connector créés pour transférer du trafic dans AWS, Azure et le Data center sont synchronisés à la plateforme ZPA

Politiques, contrôle et gestion unifiés sur AWS, Azure et les Branch Connectors

- Tableau de bord centralisé fourni dans le cloud pour la surveillance de l'intégrité des appareils et du trafic
- Filtrage disponible pour les déploiements sur Azure, AWS et les filiales
- Séries chronologiques pour les décomptes de flux et d'octets pour ZIA, ZPA, Direct, DNS

Infrastructure de journalisation consolidée pour tout type de trafic

- Journaux de session détaillés couvrant le trafic vers ZIA, ZPA et Direct (contournement Zscaler)
- Toutes les transactions DNS sont enregistrées pour les DNS publics et privés
- Entièrement intégrée à l'infrastructure NSS, la VM de pare-feu NSS peut être existante utilisée pour transmettre les journaux au SIEM

Zscaler, Inc.
120 Holger Way
San José, Californie
+1 408 533 0288
www.zscaler.com