



# Zscaler Cloud Firewall

Protection Zero Trust sécurisée et adaptative pour l'ensemble du trafic Internet

**Zscaler Cloud Firewall protège le trafic Internet de tous les utilisateurs, de toutes les applications et de tous les emplacements.**

Le monde du travail est désormais disséminé et mobile. Les applications migrent des data centers vers le cloud, tandis que les nouvelles charges de travail digitales sont de plus en plus déployées nativement dans le cloud. En outre, les utilisateurs qui travaillent depuis différents emplacements, notamment en télétravail, dans les espaces de travail partagés, les filiales et à distance, accèdent aux applications professionnelles directement depuis Internet.

Par conséquent, les utilisateurs et les applications cloud génèrent de gros volumes de trafic. Les règles de sécurité traditionnelles centrées sur le réseau, incapables de gérer la bande passante supplémentaire résultant du backhauling du trafic Internet et SaaS des utilisateurs, ont un impact sur la productivité et provoquent des congestions de la connectivité. Si les pare-feu virtuels tentent de remédier tant bien que mal à la situation, ils sont limités aux emplacements physiques des fournisseurs de services cloud, et leur administration requiert souvent des ressources dédiées de la société. Pour couronner le tout, les acteurs malveillants utilisent le chiffrement et des ports non standard pour échapper à la détection et déclencher une attaque sur les réseaux des victimes.

## Avantages de Zscaler Cloud Firewall :

- **Protection complète pour les utilisateurs en télétravail.**  
Les politiques de sécurité dynamiques basées sur les risques suivent vos utilisateurs partout, sans matrice complexe de politiques et de configurations réseau.
- **Inspection complète pour déceler les attaques cachées.**  
L'inspection illimitée du trafic inline et le déchiffrement SSL natif mettent fin aux connexions malveillantes et bloquent les menaces.
- **Détection du trafic Web évusif sur les ports non standard.**  
Identifiez et interceptez rapidement les cybermenaces évasives et chiffrées qui se cachent dans le trafic sur les ports non standard.
- **Points d'accès Internet locaux fournis dans le cloud.**  
Établissez des connexions directes à Internet rapides et sécurisées pour tout le trafic hybride et le trafic des filiales qui évoluent de manière flexible et améliorent l'expérience utilisateur.
- **Système permanent de prévention des intrusions (IPS) dans le cloud.** Les signatures IPS comportementales adaptatives, gérées par Zscaler ThreatLabz, fonctionnent en temps réel et sont simples à partager pour enrichir les flux de travail SecOps.
- **Sécurisation du DNS sans compromettre les performances.**  
Les résolutions localisées maintiennent un niveau de performance supérieur tandis que vos utilisateurs et vos terminaux sont protégés des sites malveillants et du DNS tunneling.
- **Protection fournie dans le cloud avec une présence mondiale en périphérie.**  
Zscaler Cloud Firewall procure une sécurité et une expérience utilisateur inégalées, entièrement intégrées à Zscaler Internet Access™ et faisant partie de Zscaler Zero Trust Exchange™.

Pour inspecter entièrement le trafic chiffré SSL et le trafic transitant par des ports et des protocoles non standard, les équipes chargées du réseau et de la sécurité sont souvent contraintes de sacrifier les performances et la vitesse.

Cela devient un problème dans la mesure où les pare-feu physiques peuvent rapidement atteindre leurs limites de capacité, incapables d'inspecter entièrement le trafic chiffré SSL ou les ports et protocoles non standard sans ressources supplémentaires qui affectent forcément les performances. Les pare-feu virtuels, quant à eux, sont limités aux sites physiques des fournisseurs de services cloud, et leur administration requiert souvent des ressources dédiées de l'entreprise.

## Zscaler Cloud Firewall

Pour améliorer la connectivité et la disponibilité, les entreprises doivent diriger de manière sécurisée le trafic des utilisateurs à l'aide de points d'accès Internet local, sans backhauling via des VPN et sans dupliquer la pile d'appliances de sécurité sur chaque emplacement. **Zscaler Cloud Firewall** permet au trafic Internet de circuler localement et en toute sécurité pour tous les ports et protocoles.

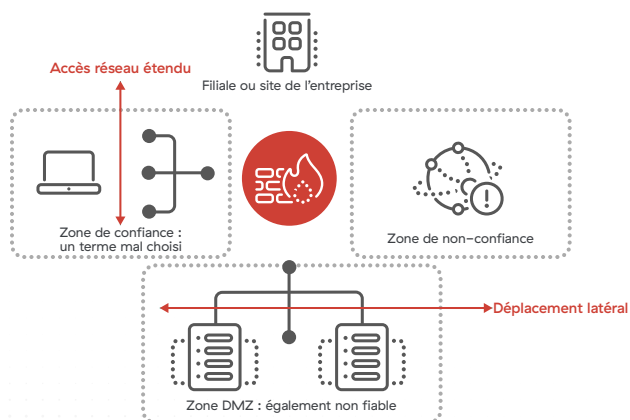
En acheminant les connexions Internet et SaaS vers Zscaler, le pare-feu Cloud-gen inspecte en mode natif tout le trafic utilisateur, y compris le trafic chiffré SSL, et s'adapte de manière flexible pour gérer des volumes élevés de connexions de longue durée.

Sans renouvellement du matériel et de mises à jour logicielles, la responsabilité des mises à jour, des mises à niveau et des correctifs, y compris les exigences d'évolutivité, pour le pare-feu basé sur le cloud, incombe à Zscaler. En supprimant les matrices complexes de politiques et de configurations réseau liées à des emplacements physiques, la gestion des politiques de pare-feu se trouve radicalement simplifiée. Grâce à des politiques adaptatives basées sur le risque qui suivent vos utilisateurs partout sur le réseau de l'entreprise et en dehors de celui-ci, Zscaler Cloud Firewall fournit une protection cohérente, quel que soit leur appareil ou l'emplacement d'où ils se connectent.

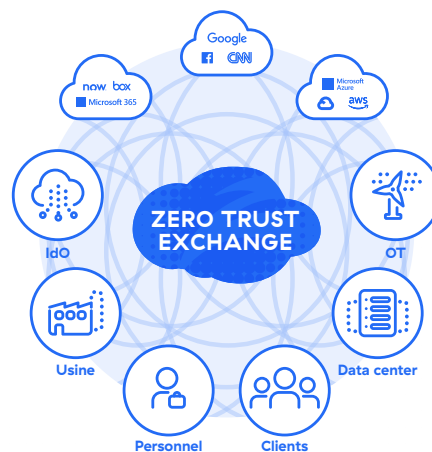
En tant qu'élément d'une fonctionnalité de pare-feu, Zscaler Cloud Firewall enregistre chaque session afin de fournir une visibilité sur l'ensemble des utilisateurs et des emplacements, ce qui vous garantit l'accès aux informations dont vous avez besoin, exactement au moment où vous en avez besoin.

## Zero Trust avec un pare-feu Cloud-Gen

### Pare-feu traditionnel – Architecture basée sur la zone



### Plateforme Zero Trust de Zscaler



En transformant vos connexions hybrides et de filiales, et en répondant dès aujourd'hui aux besoins de sécurité des performances, Zscaler prend en charge et évolue pour répondre à vos besoins de transformation vers le cloud, notamment la migration vers des applications basées sur le cloud telles que Microsoft 365.

## Avantages du pare-feu Cloud-gen

Spécialement conçu pour le monde digital moderne, Zscaler Cloud Firewall vous permet d'accéder à Internet en toute sécurité et de gérer l'ensemble du trafic Web et non Web, sur tous les ports et protocoles, avec une évolutivité flexible infinie et des performances inégalables. Vos utilisateurs bénéficient d'une protection cohérente quel que soit l'appareil qu'ils utilisent ou leur emplacement (en télétravail, au siège ou dans les filiales, ou en déplacement) sans les limitations liées au coût, à la complexité et aux performances de la sécurité réseau traditionnelle et des appliances de pare-feu de nouvelle génération.

### Alimenté par une plateforme adaptative Zero Trust

Ne faites plus de compromis avec des inspections statiques, la dégradation des performances et les limites de capacité des appliances de pare-feu physiques. Basé sur une plateforme entièrement intégrée et cloud native, Zscaler Cloud Firewall évolue de manière flexible pour gérer le trafic des

applications cloud nécessitant des connexions de longue durée, tout en interceptant et en inspectant nativement le trafic SSL/TLS, à grande échelle, afin de détecter les logiciels malveillants dissimulés dans le trafic chiffré.

### Connexions hybrides et de filiales transformatrices

Passez d'une infrastructure coûteuse et centrée sur le réseau à de véritables accès Internet locaux fournis dans le cloud. Acheminez localement le trafic Internet afin de fournir des connexions directes vers le cloud toujours rapides tout en assurant la sécurité et les contrôles d'accès pour tous les ports et protocoles. Le déploiement et la gestion d'appliances ne sont pas nécessaires, ce qui permet de réduire les coûts de backhauling MPLS et de supprimer la gestion coûteuse et fastidieuse des correctifs, la coordination des fenêtres d'interruption de service et la gestion des politiques.

### Sécurité omniprésente pour les effectifs modernes

Bénéficiez de mises à jour de sécurité en temps réel alimentées par 300 trillions de signaux quotidiens et partagées chaque jour sur l'ensemble du cloud pour une protection identique sur tout appareil, quel que soit l'endroit d'où les utilisateurs se connectent, qu'ils soient en télétravail, dans un espace de travail partagé, dans une filiale ou en déplacement. En rapprochant l'ensemble de la pile de sécurité de l'utilisateur, celui-ci bénéficie d'une protection inégalée contre les menaces, adaptée à l'utilisateur et aux applications, assortie de politiques dynamiques de suivi, sur le réseau de l'entreprise et en dehors de celui-ci.

# Gartner

Zscaler a été nommé leader du MQ SSE de Gartner, et classé au plus haut niveau en termes de « capacité d'exécution ».

En savoir plus →

### **Blocage permanent des attaques malveillantes connues**

Accomplissez ce que les solutions traditionnelles ne pouvaient pas faire avec une protection contre les menaces du système de prévention des intrusions (IPS) fournie dans le cloud et adaptée au contexte, gérée par Zscaler ThreatLabz. Grâce à une inspection illimitée du trafic inline, y compris le trafic IOT/OT et chiffré sur le réseau et en dehors de celui-ci, les signatures IPS comportementales sont appliquées en temps réel lors de l'accès à des milliers d'applications Web et non Web, quel que soit le type de connexion ou l'emplacement actuel.

### **Optimisation des DNS pour les performances et la sécurité**

Bénéficiez d'une résolution plus rapide en jumelant des applications géographiquement locales, ce qui se traduit par une meilleure expérience utilisateur et de meilleures performances des applications cloud, tout en mettant en œuvre des politiques de sécurité et de contrôle du système de noms de domaine (DNS). Les utilisateurs sont ainsi protégés contre les domaines malveillants et le DNS tunneling. En fournissant DNS en tant que service, Zscaler réduit la latence et sécurise les points d'accès à l'Internet local en utilisant des proxys complets pour tout le trafic DNS et en s'appuyant sur l'apprentissage automatique pour détecter et bloquer les activités de tunnel d'exfiltration de données.



### **Gestion simplifiée des politiques**

Définissez, déployez et appliquez immédiatement des politiques pour tous les utilisateurs, sur tous les sites, à partir d'une seule console. Au lieu des matrices complexes de politiques, de configurations de réseau et de recréation de politiques pour chaque emplacement des pare-feu typiques, le pare-feu Cloud-gen simplifie la gestion des politiques en centralisant des règles de pare-feu granulaires basées sur l'utilisateur, l'application, l'emplacement, le groupe et le département. En outre, les administrateurs peuvent envoyer des journaux complets et détaillés sur les utilisateurs, les demandes, les réponses, les services utilisés, etc. aux outils SIEM et XDR afin d'améliorer les enquêtes de sécurité et la réponse aux incidents.

## **Caractéristiques principales du pare-feu Cloud-gen**

<b>Gestion centralisée des politiques</b>	Définissez et appliquez immédiatement les politiques sur tous les sites sans avoir à recréer des politiques pour chaque emplacement.
<b>Services de sécurité entièrement intégrés</b>	Les informations contextuelles sont partagées entre les services DLP, APT, sandbox et autres pour offrir une meilleure protection et une plus grande visibilité.
<b>Contrôle granulaire, journalisation et visibilité en temps réel</b>	Une journalisation enrichie pour une visibilité détaillée, avec une journalisation unifiée au niveau mondial et illimitée pendant six mois, permettant l'analyse et la corrélation pour dégager des tendances, analyser la productivité et résoudre les problèmes.
<b>Protection contre les menaces en fonction de l'utilisateur</b>	Définissez les utilisateurs par groupes, départements ou sites, notamment en définissant le télétravail ou les utilisateurs distants en tant qu'emplacement, et intégrez les fournisseurs d'identité et les bases de données d'utilisateurs locaux, ce qui permet d'appliquer des politiques cohérentes quel que soit l'emplacement physique des utilisateurs.

## Caractéristiques principales du pare-feu Cloud-gen (suite)

<p><b>Protection contre les menaces en fonction des applications</b></p>	<p>Identifiez et classez les services applicatifs dès le premier paquet pour activer les politiques de filtrage et de transfert du pare-feu, en prenant de mesures immédiates et de plus haute priorité avec des politiques adaptatives et contextuelles.</p> <p>Les types d'applications dans tous les services réseau sont pris en charge : ports et protocoles, applications réseau ; SNI (nom d'hôte), services basés sur le DPI, services applicatifs ; UCaaS basé sur l'identification du premier paquet, IP, groupes FQDN et autres détections basées sur l'heuristique.</p>
<p><b>Sécurité et contrôle IPS adaptatifs</b></p>	<p>Assurez une protection permanente fournie dans le cloud contre les menaces avec des signatures IPS personnalisées et des milliers de signatures IPS adaptatives et comportementales sur n'importe quel port et protocole, quel que soit le type de connexion ou l'emplacement, en inspectant tout le trafic Internet de l'utilisateur. <b>Consultez la liste de toutes les signatures IPS gérées par ThreatLabZ.</b></p>
<p><b>Inspection de sécurité avancée</b></p>	<p>Effectuez une inspection complète des paquets sur les protocoles non Web, notamment FTP, DNS, RDP, Telnet, etc. pour identifier et empêcher le trafic évusif sur les ports non standard.</p>
<p><b>Sécurité et contrôle DNS</b></p>	<p>Optimisez les performances des applications cloud et minimisez la latence tout en garantissant une sécurité sans compromission en faisant passer tous les DNS par Zscaler. Activez des politiques basées sur l'utilisateur, l'application, l'emplacement et le pays de l'IP résolue pour bloquer automatiquement les utilisateurs provenant de domaines malveillants, et pour détecter et empêcher le DNS tunneling.</p> <p><b>Résolution :</b> le DNS en tant que service fournit une résolution optimale avec la localisation, l'entité et la latence la plus faible.</p> <p><b>Filtrage DNS :</b> créez des règles de filtrage DNS personnalisées pour bloquer, autoriser ou rediriger différents types de requêtes DNS vers des destinations connues et malveillantes.</p> <p><b>Sécurité et exfiltration de données :</b> détectez les logiciels malveillants, l'hameçonnage, le DNS tunneling et l'exfiltration de données à l'aide de l'apprentissage automatique.</p> <p><b>DNS over HTTPS (DoH) :</b> empêchez les angles morts du DoH et le contournement des contrôles organisationnels lors du chiffrement des connexions DNS dans le trafic HTTP commun.</p>
<p><b>Politiques de nom de domaine pleinement qualifié (FQDN)</b></p>	<p>Configurez et gérez facilement les politiques d'accès pour les applications hébergées sur plusieurs adresses IP.</p>
<p><b>Contrôle du protocole de transfert de fichiers (FTP) et prise en charge du NAT (Network Address Translation)</b></p>	<p>Le contrôle d'accès FTP et FTP over HTTP, ainsi que la prise en charge du proxy de destination NAT et de la redirection NAT sont disponibles.</p>
<p><b>Certifications de confidentialité et de conformité</b></p>	<p>Assurez le respect des normes internationales les plus strictes en matière de risques, de confidentialité et de conformité pour les entreprises et les gouvernements.</p> 
<p><b>Réglementations relatives à l'industrie et à la confidentialité des données</b></p>	<p>Assurez le respect des réglementations sectorielles et nationales en matière de confidentialité des données.</p> 
<p><b>Protection mondiale partagée</b></p>	<p>Bénéficiez de l'effet cloud : chaque fois qu'une nouvelle menace est identifiée dans une des dizaines de milliards de transactions traitées quotidiennement par Zscaler Cloud, tous les utilisateurs de Zscaler, où qu'ils soient, en sont protégés.</p>

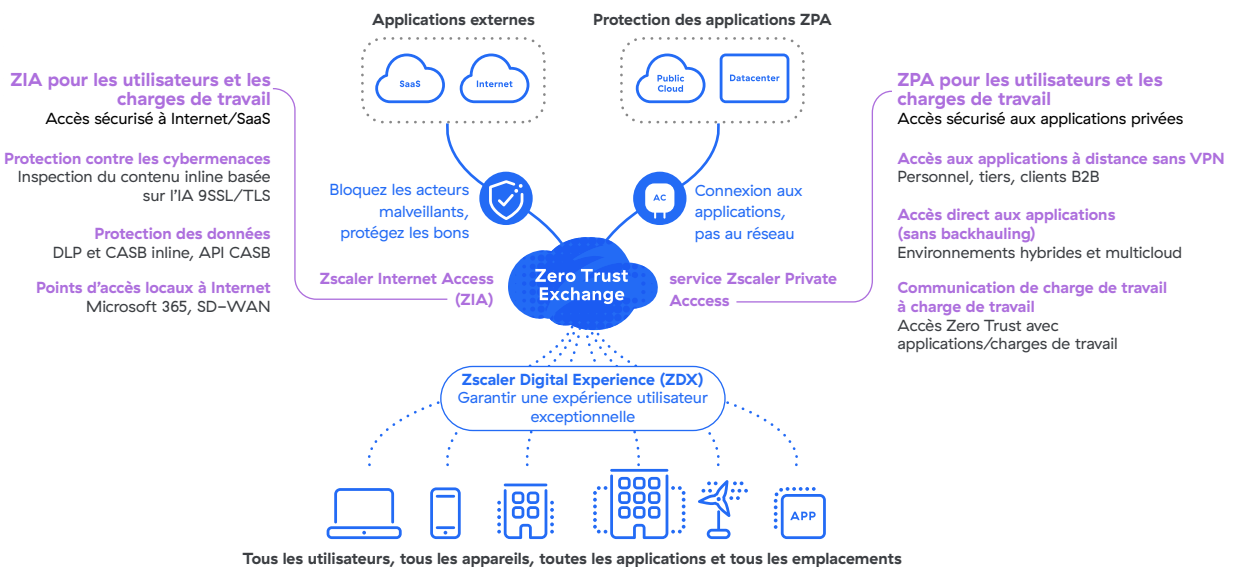


## Zscaler Cloud Firewall est entièrement intégré à Zscaler Internet Access™ et fait partie du Zero Trust Exchange global

Zscaler Zero Trust Exchange facilite des connexions rapides et sécurisées et permet à vos employés d'adopter le télétravail en utilisant Internet comme réseau d'entreprise. Avec pour fondement le principe Zero Trust de l'accès sur la base du moindre privilège, il fournit une sécurité complète en utilisant l'identité basée sur le contexte et l'application des politiques.

### Comment Zscaler fournit une politique Zero Trust aux utilisateurs, aux charges de travail et à l'IIoT/OT

Effectuer le déploiement en quelques semaines pour améliorer la cyber-protection et l'expérience utilisateur



Experience your world, secured.™

#### À propos de Zscaler

Zscaler (NASDAQ : ZS) accélère la transformation digitale de sorte que les clients deviennent plus agiles, plus efficaces, plus résilients, avec une meilleure sécurité. La plateforme Zscaler Zero Trust Exchange protège des milliers de clients contre les cyberattaques et la perte des données en connectant de manière sécurisée les utilisateurs, les appareils et les applications indépendamment de l'emplacement. Distribué à travers plus de 150 data centers dans le monde, Zero Trust Exchange basé sur SASE est la plus grande plateforme de sécurité cloud inline. Pour en savoir plus, rendez-vous sur [zscaler.fr](https://zscaler.fr) ou suivez-nous sur Twitter [@zscaler](https://twitter.com/zscaler).

©2022 Zscaler, Inc. Tous droits réservés. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, Zscaler Private Access™, ZIA™, ZPAT™ et les autres marques commerciales répertoriées sur [zscaler.fr/legal/trademarks](https://zscaler.fr/legal/trademarks) sont soit 1) des marques déposées ou des marques de service, soit 2) des marques déposées ou des marques de service de Zscaler, Inc. aux États-Unis et/ou dans d'autres pays. Toutes les autres marques commerciales sont la propriété de leurs détenteurs respectifs.