



# Zscaler Cloud Firewall

Les clés d'une migration sécurisée vers le cloud



## Exploitez les atouts de Zscaler Cloud Firewall lors de votre migration vers le cloud

Le phénomène de migration des applications vers le cloud à l'aide de protocoles Web n'est pas nouveau. Chez Zscaler, nous avons anticipé ce changement lorsque nous démarrions la construction de notre système de sécurité cloud en 2008. Aujourd'hui, notre cloud extrêmement évolutif nous offre la flexibilité nécessaire pour inspecter le trafic et explorer les données des sessions HTTP et HTTPS.

À mesure que les applications émigrent des data centers centralisés, le modèle de backhaul centralisé devient problématique: en plus d'être coûteux, il ralentit l'expérience utilisateur. Par exemple, si vous acheminez le trafic DNS via un firewall traditionnel installé sur un site centralisé, la réponse se fera au niveau du firewall et non de l'utilisateur, affectant les performances en temps réel des applications.

Puissants catalyseurs métier, les applications cloud présentent néanmoins leurs propres défis. [Office 365](#) par exemple ouvre plusieurs connexions par utilisateur, entraînant l'augmentation de la consommation de la bande passante et la saturation des capacités des ports et du débit des firewalls traditionnels. Une [récente enquête](#) effectuée à l'initiative de Zscaler sur les effets du déploiement d'Office 365 a révélé que les problèmes de réseau et de latence étaient courants. De nombreuses organisations ont mis à niveau leurs firewalls avant le déploiement, mais 69% ont toujours signalé une augmentation de la latence après le déploiement. Augmenter la bande passante du trafic en backhauling n'a pas non plus suffi pour résoudre le problème. Soixante-neuf pour cent des personnes sondées ont signalé des problèmes hebdomadaires et 30 pour cent des problèmes quotidiens de performance.

## Avantages de Zscaler Cloud Firewall

[Zscaler Cloud Firewall](#) relève ces défis de la même manière que le proxy cloud améliore le trafic Web. Il permet la mise en place des points d'accès locaux à Internet rapides et sécurisés pour tous les ports et protocoles, sans aucune mise à niveau ou déploiement d'appareils, le tout géré de manière centralisée. Zscaler Cloud Firewall, comme le reste de la plate-forme Zscaler, évolue de manière élastique avec votre consommation, et vos coûts sont strictement basés sur le nombre d'utilisateurs.

Avec Zscaler, les politiques ne sont pas liées à un emplacement physique. Elles accompagnent plutôt les utilisateurs pour leur fournir une protection identique quel que soit l'appareil qu'ils utilisent ou le lieu depuis lequel ils se connectent. Les responsables de votre entreprise bénéficient donc des mêmes accès et protections, qu'ils travaillent au siège social, visitent des filiales ou assistent aux réunions dans le monde entier.

Zscaler propose deux services de cloud firewall: un Cloud Firewall standard inclus dans chaque abonnement Zscaler Internet Access et une mise à niveau avancée du cloud Firewall incluse dans le package de transformation, ou pouvant être achetée à part.

## Quelle est la différence entre les Cloud Firewall "standard" et "avancé"?

L'offre standard de Zscaler Cloud Firewall est incluse dans votre abonnement aux services Zscaler Internet Access. La description qui va suivre comprend certaines des fonctionnalités de politique qui sont déjà à votre disposition. Nous décrirons également l'offre avancée de Zscaler Cloud Firewall, un service inclus dans l'ensemble de transformation, qui peut également être acheté à part, en tant que mise à niveau.

## Intéressons-nous d'abord aux politiques communes aux deux produits

### FIREWALL CLOUD STANDARD

Appliquez une politique de sécurité autoriser/bloquer basée sur l'adresse IP source et de destination des ports et des protocoles. Les fonctionnalités suivantes sont disponibles pour tout votre trafic sortant:

- Politique unifiée (règles quintuple par emplacement)
- Console d'administration unique
- Un ensemble unique de journaux sur tous vos sites et utilisateurs

### FIREWALL CLOUD AVANCÉ

Appliquez des politiques de sécurité détaillées de type autoriser/bloquer en fonction des applications utilisant un moteur Deep Packet Inspection (DPI):

- Toutes les fonctionnalités de l'offre Zscaler Cloud Firewall standard
- Bénéficiez de tous les avantages d'un pare-feu nouvelle génération (NGFW) – ainsi que l'intelligence et la gestion du cloud Zscaler – sans avoir à acheter ou à maintenir des appliances coûteuses
- Sécurité et contrôle DNS: Optimisez la résolution DNS et fournissez des contrôles détaillés permettant de détecter et d'empêcher le tunnelling DNS
- NGFW et politiques contextuelles: Accès et politiques de sécurité granulaires de type autoriser/bloquer définis en fonction des applications, de l'identité de l'utilisateur, du groupe et de l'emplacement
- Politiques de noms de domaine pleinement qualifiés: Politiques d'accès pour les applications hébergées à plusieurs adresses IP
- Tableau de bord complet: Il permet une visibilité en temps réel sur l'utilisation du trafic, les menaces et les applications pour chaque utilisateur, groupe ou emplacement
- Journalisation et rapports complets pour chaque session
- Cloud IPS: Offrez une protection permanente contre les menaces des systèmes de prévention d'intrusion (IPS) ainsi qu'une visibilité complète quel que soit le type de connexion ou l'emplacement. Inspectez tout le trafic Internet des utilisateurs (y compris en SSL)
- Transfert automatique de proxy pour les ports non standard: Identifiez et sécurisez automatiquement les applications qui utilisent des ports et des protocoles non standard

Pour contrer une attaque basée sur un protocole et utilisant des numéros de protocole connus, l'offre standard de Zscaler Cloud Firewall suffira probablement. Elle vous permet par exemple d'empêcher l'utilisation d'un autre serveur DNS en bloquant le port 53.

Mais que se passe-t-il si une application a le bon numéro de port, mais n'est pas celles que vous pensez? De la même manière que le proxy est devenu incontournable pour les applications s'exécutant en HTTP et HTTPS, si vous souhaitez accéder à des informations plus approfondies, il vous faudra un cloud Firewall avancé. Si vous souhaitez savoir quel processus utilise un port que vous avez ouvert et ce que vos utilisateurs essaient de faire, vous devez passer à la version avancée de Zscaler Cloud Firewall.

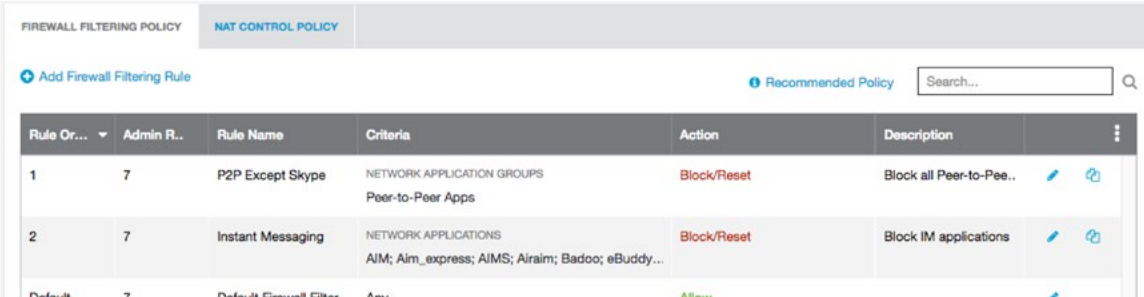
## Repenser la politique

Le passage des listes de contrôle d'accès (ACL) aux firewalls dynamiques, puis aux systèmes NGFW n'a rien changé au fonctionnement de base. Nous voulions "faire des trous" dans le firewall pour y autoriser le trafic que nous jugions acceptable et bloquer tout le reste. La règle "tout bloquer" figure à la fin de presque tous les ensembles de règles de firewall existants.

Bien qu'il s'agisse toujours d'un modèle de conception valide, il est peut-être temps de repenser ce modèle pour ce qui est du trafic sortant de l'organisation. Il vaut la peine d'envisager de changer votre dernière règle en "tout autoriser". Cette approche permet de bloquer ce que vous ne voulez pas tout en permettant à tout le reste du trafic de se poursuivre normalement.

Pourquoi changer une approche qui a fonctionné et qui de surcroît est recommandée depuis des décennies par des experts en sécurité? Eh bien, parce qu'au cours des 20 dernières années, la nature de notre travail a complètement transformé la façon dont nous utilisons Internet.

Aujourd'hui les exigences en termes de politiques ou de réglementation varient d'une organisation à l'autre et peuvent influencer la décision de bloquer ou d'autoriser tout le trafic. Comment pouvez-vous donc décider quelle choix vous convient le mieux? Analyser le fonctionnement de votre organisation et les services que vous fournissez vous aidera à faire le bon choix.



Rule Or...	Admin R..	Rule Name	Criteria	Action	Description
1	7	P2P Except Skype	NETWORK APPLICATION GROUPS Peer-to-Peer Apps	Block/Reset	Block all Peer-to-Pee..
2	7	Instant Messaging	NETWORK APPLICATIONS AIM; Aim_express; AIMS; Airaim; Badoo; eBuddy...	Block/Reset	Block IM applications
Default	7	Default Firewall Filter...	Any	Allow	

Fig 1. Exemple d'une règle par défaut de type "tout autoriser"

Si vous offrez un réseau ouvert dans un espace public, vous opterez probablement pour la règle "tout autoriser" après avoir bloqué le contenu inacceptable et empêché les potentielles activités malveillantes ou illégales en bloquant les protocoles tels que le P2P. Étant donné que les utilisateurs d'un réseau public accèdent à Internet et non à votre data center, le reste du trafic est susceptible d'être acceptable pour votre organisation.

Rule Or...	Admin R...	Rule Name	Criteria	Action	Description	...
1	7	DNS-Rule	NETWORK SERVICES DNS	Allow	Allow DNS	
2	7	Allow-Web-Traffic	NETWORK SERVICES HTTP, HTTPS TIME Work-Hours	Allow	Allow the use of HTT...	
3	7	File-Transfers	DEPARTMENTS IT; IT Networking; IT Security NETWORK APPLICATIONS TFTP; FTPS; FTP-Data; FTP	Allow	Allow IT users to use...	
4	7	Office-365	DEPARTMENTS Engineering; Engineering QA; Executive; Finance... NETWORK APPLICATION GROUPS Microsoft Office365	Allow	Allow Office 365 for ...	
5	7	Finance-AWS-Test-S...	DEPARTMENTS Finance DESTINATION ADDRESSES finance-aws.safemarch.com	Allow	Allow finance to use ...	
6	7	Azure Server Access	DEPARTMENTS IT DESTINATION ADDRESSES mycompanyapp.azure.com	Allow	IT access to Azure s...	
7	7	Developer-Access	DEPARTMENTS Engineering Development; Research & Developm... DESTINATION ADDRESSES github.com; stackexchange.com	Allow	Allow access to Dev ...	
Default	7	Default Firewall Filte...	Any	Block/Reset		

Fig 2. Exemple d'une règle par défaut de type "tout bloquer"

Toutefois, si votre organisation appartient à un secteur hautement réglementé, comme le secteur de la santé ou la banque, vous souhaiterez peut-être n'autoriser que les applications approuvées. Dans ce cas, l'approche la plus appropriée est d'ouvrir la voie au trafic autorisé et de bloquer tout le reste en local. Seules les applications qui ont besoin d'un accès Internet pour fonctionner devrait être autorisée, et la règle "tout bloquer" serait la meilleure façon de conclure votre politique.

Pour plus d'informations sur Zscaler Cloud Firewall et comment le configurer, commencez par consulter notre documentation ici: <https://help.zscaler.com/zia/about-firewall-control>

## Conclusion

Le lieu de travail évolue rapidement. L'avenir verra les data centers être remplacés par des infrastructures et services cloud. Les backhails coûteux sont remplacées par des points d'accès locaux. Les utilisateurs quant à eux travaillent de plus en plus en dehors du réseau de l'entreprise, loin du bureau. Pour sécuriser cette nouvelle norme, il vous faut une plate-forme de sécurité avec des services et des politiques intégrés qui accompagnent les utilisateurs peu importe leur emplacement et la manière dont ils souhaitent travailler. Zscaler Cloud Firewall permet la mise en œuvre des points d'accès à Internet locaux rapides et sécurisés pour tous les ports et protocoles, sans aucune appliance. La plate-forme Zscaler Cloud Security Platform associée à la solution cloud Firewall standard rapproche l'ensemble de la pile de sécurité de l'utilisateur pour lui assurer une protection identique, peu importe où il se connecte, et évolue de manière élastique pour gérer tout le trafic lié à votre application cloud.