Pare-feu traditionnel vs Pare-feu cloud

Cinq raisons pour migrer

67 % des administrateurs réseau s'accordent à penser que les pare-feux traditionnels ne peuvent fournir un accès rapide et sécurisé aux utilisateurs à distance.[1] Quelles sont les différences par rapport à un pare-feu cloud.

Pare-feu traditionnel vs **Pare-feu cloud**

1 Accès et sécurité

Les pare-feux traditionnels entraînent des risques pour votre entreprise en raison d'un accès sans restriction.

La confiance implicite (accordée par défaut) peut aboutir à un accès libre et à un risque de **déplacement en interne des menaces.**

90 % des administrateurs IT et de sécurité admettent avoir appliqué des politiques très permissives[2].

Les pare-feux cloud-native assurent une connexion sécurisée* et sans interruption de service.

* Avec une approche Zero Trust

Facile à comprendre, la gestion centralisée des politiques minimise les erreurs de configuration et facilite leur résolution.

La protection fournie par le cloud garantit l'application des politiques par rapport aux utilisateurs présents au sein et à l'extérieur du réseau, via des connexions transparentes.

2 Expérience utilisateur et évolutivité

Les pare-feux traditionnels ralentissent les utilisateurs finaux et ne réalisent aucune inspection TLS/SSL.

L'inspection de l'ensemble du trafic peut **ralentir les performances à hauteur de 50 %.**

Face à un volume de trafic important, vous devez disposer **de capacités plus importantes et de davantage d'appliances** dans votre data centre — Les capacités des pare-feux virtuels restent limitées au même titre que celles des boîtiers physiques.

Les pare-feux cloud-native assurent des inspections illimitées et sans latence.

Véritables points d'accès en local vers Internet et fournis depuis le cloud pour des connexions directes à Internet.

Le moteur Zscaler Single-Scan, Multi-Action™ (SSMA) analyse l'ensemble des données et du trafic, notamment sur SSL/TLS, pour appliquer en mode inline, la fonction de sécurité la plus pertinente, sans peser sur les performances.

3 Coût[3]

Les pare-feux traditionnels engendrent un investissement et des coûts de fonctionnement élevés.

+30 000 à 250 000 € par dispositif professionnel — En général, chaque site nécessite le déploiement de 2 appareils.

Plus de 50 000 € par an pour la gestion, en plus du coût du matériel, des logiciels et des mises à jour des signatures.

Les pare-feux cloud-native encouragent de des économies majeures.

Pas de matériel ni de logiciel à gérer, uniquement des licences

Zscaler restreint le nombre d'appareils **de 90 %** et permet de réduire les équipes de support de **74 % en ETP**[4].

4 Zero Trust

Les pare-feux traditionnels ne sont pas adaptés au Zero Trust.

- Déploie un protocole strict d'authentification des utilisateurs
- Garantit l'intégrité et la sécurité des ressources
- Modifie les politiques en temps réel en cas de changement de comportement ou d'environnement

Les pare-feux cloud-native proposent le Zero Trust.

- Authentification stricte et permanente des utilisateurs et contrôles des politiques
- Vérifie le contexte et détermine la posture de sécurité et les risques associés aux dispositifs et aux utilisateur
- Établit des connexions directes et sécurisées entre l'utilisateur et l'application

5 Gestion

Les pare-feux traditionnels sont gourmands en ressources

75 % des administrateurs réseau révèlent qu'il est difficile de gérer les pare-feux matériels, leurs mises à niveau et leur déploiement[5].

Plus de temps à consacrer aux correctifs, aux mises à jour, au déploiement, à la recherche, à la remédiation et au monitoring.

Les pare-feux cloud-native permettent de consacrer plus de temps aux tâches essentielles.

Pas de correctifs, de mise à niveau, de déploiement ou configuration excessive de la fonction IPS avec FWaaS.

Il est possible de réduire de 74 % le temps consacré à la maintenance **afin de se recentrer sur des objectifs plus stratégiques.**

Vous souhaitez passer à l'action et router votre trafic vers un pare-feu cloud-native ? Pour vous lancer, consultez le rapport d'IDC *Why True Security Transformation Requires Cloud Firewalls*.

Consulter le rapport

1. Virtual Intelligence Briefing (VIB), Enquête de 2021 sur la sécurité des réseaux
2. Zscaler, 7 Symptoms Your Legacy Firewall Isn't Zero Trust Compatible
3. Données rapportées par les clients de Zscaler
4. Zscaler et IDG, Rapport de validation économique, 2021
5. Source : Virtual Intelligence Briefing (VIB), Enquête de 2021 sur la sécurité des réseaux

zscaler | Experience your world, secured.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408 533 0288
www.zscaler.fr