Barracuda CloudGen Firewall

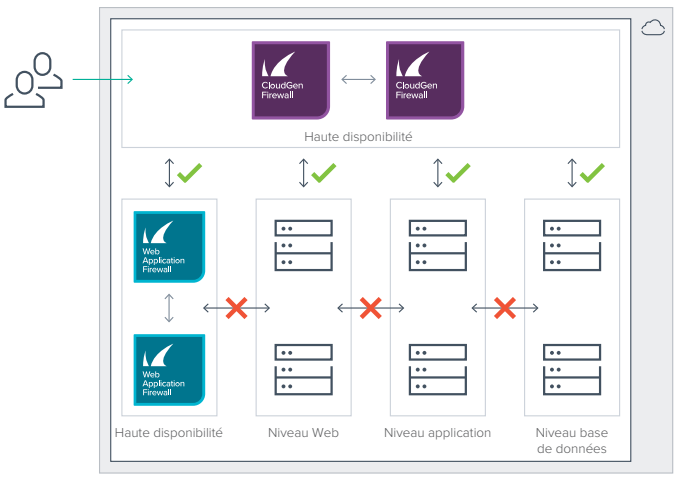
Segmentation du réseau et surveillance des charges de travail élastiques dans le cloud public

L'augmentation du nombre de migrations vers le cloud contribue à la hausse de la demande de mesures de sécurité avancées, non seulement dans le cloud, mais également pour les architectures hybrides qui conservent les applications et les données essentielles sur des serveurs sur site à des fins de conformité ou autres.

Les pare-feu Barracuda CloudGen Firewall segmentent les réseaux en plusieurs niveaux et sécurisent, limitent et surveillent les communications entre ces niveaux. Vous bénéficiez ainsi d'une sécurité renforcée ainsi qu'un certain degré de visibilité et de conformité pour les applications hébergées dans les environnements de cloud public. De plus, les capacités de VPN et de SD-WAN robustes vous permettent de vérifier que les mêmes niveaux de sécurité et de visibilité sont appliqués dans les niveaux de réseau sur site et dans le cloud. En outre, ces capacités optimisent les performances et réduisent considérablement les coûts de votre système.

Optimisation de la méthode « Lift and shift »

Il se peut qu'à l'instar des autres entreprises vous effectuiez un processus de déplacement ou de réplication d'un grand nombre de vos anciennes charges de travail vers le cloud. Dans le contexte actuel des nombreuses préoccupations relatives à la sécurité, vous appliquez certainement des normes de sécurité plus strictes aux données dans le cloud qu'à vos centres de données sur site.



Pour ce faire, la méthode la plus efficace est d'appliquer une segmentation stricte du réseau en plusieurs niveaux. Vous disposerez ainsi d'un certain degré de sécurité, de visibilité et de conformité pour les applications hébergées dans le cloud public. Les pare-feu Barracuda CloudGen Firewall sont conçus pour les environnements cloud natifs suivants :

- Sécurité et confinement améliorés - Le trafic réseau est isolé et filtré à l'aide d'un système de prévention des intrusions (IPS), d'un anti-malware et du dispositif Advanced Threat Protection pour le protéger contre la propagation d'attaques ou de dangers dans les niveaux de réseau dans le cloud.
- Contrôle des accès - Des contrôles granulaires sont appliqués pour permettre à chaque utilisateur d'accéder uniquement à des ressources spécifiques du réseau dans le cloud.
- Visibilité et surveillance du réseau en temps réel - Ce dispositif vous permet de surveiller les connexions internes autorisées et refusées et de lancer des alertes sur ces dernières. Vous pouvez également détecter les comportements suspects et consigner les événements pour les analyser ultérieurement.
- Confinement immédiat - Lorsqu'un problème de réseau survient, il ne se répercute qu'au niveau du sous-réseau local ou de l'hôte individuel subissant le problème.
- Intégration WAF - Le WAF de Barracuda CloudGen est un outil privilégié pour la détection d'attaques complexes visant la couche application. Cet outil est d'une efficacité redoutable pour bloquer les connexions et les attaques menaçant la couche application. Lorsque Barracuda CloudGen WAF décèle une tentative de piratage, les connexions de la source de l'attaque sont synchronisées au Barracuda CloudGen Firewall pour bloquer toutes les connexions réseau qui se trouvent déjà sur la couche réseau. Cela permet de libérer des ressources sur le WAF CloudGen et d'améliorer les performances de l'application protégée.

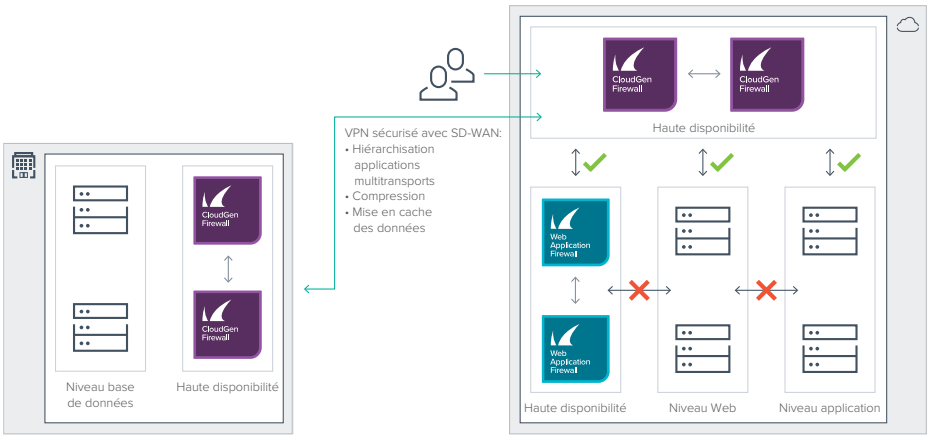
Conformité aux réglementations et avantages du cloud

Pour des raisons de conformité, certaines charges de travail, comme les serveurs de base de données contenant des données sensibles, doivent être hébergées sur site tandis que les serveurs d'applications et les serveurs Web sont hébergés dans le cloud public. Cela génère un risque de goulet d'étranglement entre le niveau de réseau dans le cloud et le niveau de réseau sur site. Qui plus est, les potentielles économies réalisées du fait de la transition vers le cloud public diminueront. En outre, cette situation ajoute un certain degré d'incertitude quant à la disponibilité des applications.

Si vous vous appuyez sur des liaisons montantes haute performance dédiées pour assurer l'efficacité et la disponibilité, les tarifs peuvent augmenter de façon exponentielle. Par ailleurs, cette solution ne règle pas non plus la question de l'incertitude concernant la disponibilité des applications en cas de panne de la liaison montante.

Les pare-feu de Barracuda CloudGen Firewall optimisent les VPN sécurisés sur le cloud public et proposent des fonctions SD-WAN complètes pour en améliorer les performances. Vous pouvez améliorer les lignes louées onéreuses ou remplacer ces dernières par plusieurs liaisons Internet montantes à large bande peu coûteuses, qui ont été rassemblées pour acheminer des tunnels VPN sécurisés vers le cloud. En cas de panne de liaison montante, Barracuda CloudGen Firewall bascule les sessions vers les liaisons restantes de façon instantanée et transparente, et ce sans perte de session ni interruption de travail. Pour optimiser les performances de l'application, les pare-feu Barracuda CloudGen Firewall effectuent de manière proactive des mesures de bande passante et de latence disponibles entre les terminaux VPN pour chacune des liaisons physiques montantes vers le cloud public, et modifie les flux de trafic selon ces mesures.

Les fonctions de compression de trafic, de déduplication des données et de mise en cache au sein de la connexion VPN permettent de réduire considérablement les exigences en matière de bande passante des liaisons montantes et de faire baisser les coûts par la même occasion.



Connectivité de cloud à cloud permanente

Pour des raisons de conformité, certaines charges de travail, comme les serveurs de base de données contenant des données sensibles, doivent être hébergées sur site tandis que les serveurs d'applications et les serveurs Web sont hébergés dans le cloud public. Cela génère un risque de goulet d'étranglement entre le niveau de réseau dans le cloud et le niveau de réseau sur site. Qui plus est, les potentielles économies réalisées du fait de la transition vers le cloud public diminueront. En outre, cette situation ajoute un certain degré d'incertitude quant à la disponibilité des applications.

Les pare-feu de Barracuda CloudGen Firewall permettent aux entreprises d'utiliser plusieurs charges de travail dans le cloud en même temps, même si elles sont hébergées par différents fournisseurs. La technologie SD-WAN sécurisée et l'extension de protocole VPN propriétaire « TINA » haute performance sont disponibles pour tous les fournisseurs de services dans le cloud ainsi que pour les déploiements virtuels et sur site. Grâce à ces dispositifs, il est possible de s'affranchir des limites des connexions IPsec traditionnelles pour garantir une connectivité permanente avec tous les fournisseurs d'infrastructure cloud.

Synthèse

Les pare-feu Barracuda CloudGen Firewall offrent une combinaison unique de dispositifs de sécurité de nouvelle génération, de SD-WAN sécurisé, d'intégration au cloud et d'optimisation de trafic intelligente pour sécuriser l'adoption du cloud public. La segmentation des réseaux en plusieurs niveaux vous permet d'obtenir un certain degré de sécurité, de visibilité et de conformité pour les applications hébergées dans le cloud public. Les pare-feu Barracuda CloudGen Firewall sécurisent et surveillent les communications entre ces niveaux tout en réduisant les éventuels dégâts subis par votre entreprise en cas d'attaque. En construisant des ponts entre infrastructure cloud, sécurité et stratégie de défense en profondeur, Barracuda vous propose une protection entre les couches application et données de votre réseau.

Barracuda
Your journey, secured.