PRÉSENTATION DE LA SOLUTION AKAMAI

Gestion des accès et des identités utilisateur avec la segmentation

Un niveau de contrôle supplémentaire essentiel pour les centres de données hybrides contemporains

Réduire la surface d'attaque des environnements informatiques d'aujourd'hui ne se limite pas à créer des contrôles stricts concernant des applications spécifiques pour les protéger des dangers. Cette première étape est un bon début et peut certainement être utile dans certains cas, tels que le confinement des violations ou la conformité. Cependant, sans solution de segmentation prenant en charge la gestion des accès et des identités utilisateur, votre entreprise compte un angle mort en matière de sécurité qui concerne chaque personne qui utilise votre réseau ou y accède.

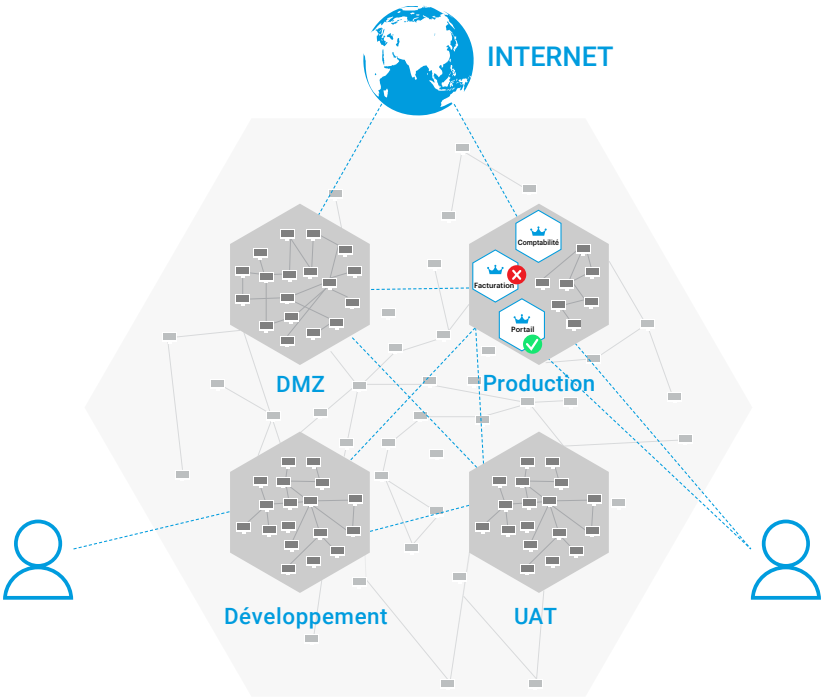
Une fois la segmentation des applications en place, l'étape essentielle suivante consiste à utiliser votre solution de segmentation pour créer une règle concernant les personnes autorisées à accéder à ces applications, veillant ainsi à ce que ces dernières soient sécurisées sur toutes les architectures de votre réseau.

Scénarios d'utilisation : segmentation pour les accès et les identités utilisateur

Gérer les accès utilisateur

Grâce à un groupe d'utilisateurs Active Directory, Akamai Guardicore Segmentation peut contrôler les accès utilisateur à toute application ou charge de travail, depuis n'importe quel environnement. Des groupes d'utilisateurs spécifiques ont accès à des serveurs spécifiques, via des ports ou des processus spécifiques, tandis que d'autres n'y ont pas accès. Ces groupes d'utilisateurs disposent de leurs propres autorisations, tandis que tout autre accès peut être bloqué. Sans avoir besoin d'un pare-feu centralisé, vous pouvez utiliser un contrôle d'accès granulaire entre les charges de travail sur des segments spécifiques du réseau.

Contrôle des accès utilisateur



Pourquoi choisir la segmentation pour le contrôle des accès utilisateur ?

Contrôle des accès utilisateur partout
Les règles fonctionnent sur les ordinateurs portables, les ordinateurs de bureau, les environnements VDI, les serveurs virtuels ou dédiés physiques (bare metal) et les infrastructures cloud

Segmentation logicielle
Aucune modification de réseau ou d'architecture, aucun câble, aucun temps d'arrêt des serveurs et aucun redémarrage des systèmes

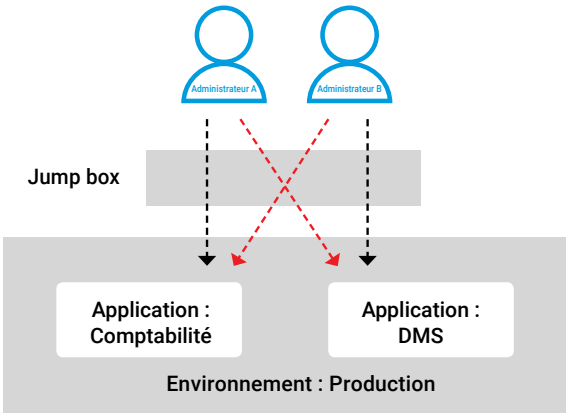
Rapidité et efficacité
Simples et intuitives à créer, les règles s'appliquent immédiatement sur les sessions nouvelles et actives

Rentabilité
Par rapport à des cas d'utilisation similaires rencontrés avec une infrastructure de jump box traditionnelle, les coûts sont jusqu'à 60 % inférieurs

Akamai

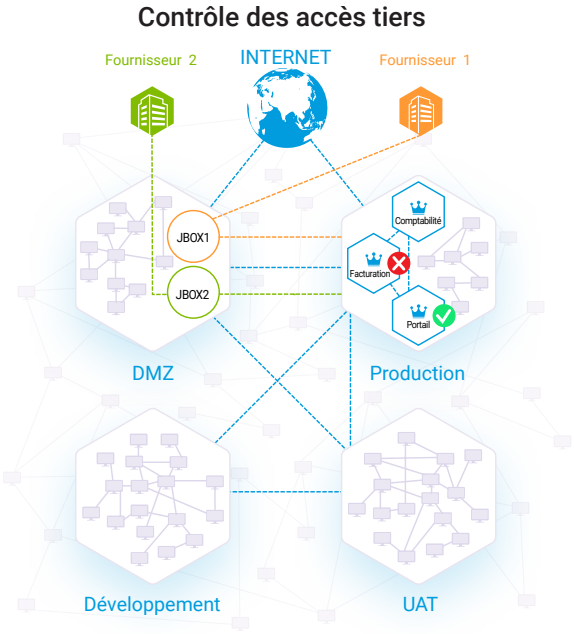
Gérer les accès utilisateur simultanés

Les administrateurs peuvent accéder à différentes applications via le même serveur de terminal ou de jump box, même lorsqu'ils y sont connectés en même temps. Des règles disparates s'appliqueront en toute transparence, permettant ainsi à un utilisateur d'accéder aux applications auxquelles il est autorisé à accéder, tandis qu'un autre restera bloqué, sans interruption du service ou de l'accès propre à l'un ou l'autre des utilisateurs.



Contrôler les accès tiers

En fonction des identités utilisateur, Akamai Guardicore Segmentation peut contrôler la gestion des accès tiers (fournisseurs externes ou SaaS, par exemple). Avec l'aide de groupes d'utilisateurs, chaque connexion tierce peut avoir ses propres règles d'accès définies pour le centre de données et des applications spécifiques, accordant ainsi des autorisations à l'utilisateur pour ce dont il a besoin dans le cadre de ses fonctions, et rien de plus.



Ensemble, la segmentation des applications et la gestion des accès et des identités utilisateur permettent de protéger efficacement les centres de données d'entreprise d'aujourd'hui.

Vous voulez en savoir plus sur la façon dont ces méthodes fonctionnent en tandem ? Contactez-nous pour discuter avec l'un de nos experts.