tufin The Security Policy Company. + aws

Bénéfices de la solution Tufin pour AWS

Visibilité, conformité et automatisation pour Amazon Web Services (AWS)

Avantages pour votre entreprise:

- Gain de visibilité et sécurité sur AWS et les réseaux hybride d'entreprise
- Plus grande agilité grâce à une orchestration des politiques de sécurité couvrant le cloud et l'infrastructure locale
- Automatisation des opérations de sécurité pour AWS afin de mettre en place des contrôles intégrés
- Assurance d'une segmentation renforcée et d'une conformité constante aux stratégies sur AWS et au travers du réseau hybride
- Réduction de près de 70 % du temps lié aux vérifications grâce à l'analyse de conformité permanente
- Dépannage et mise à disposition de la connectivité nord-sud pour les applications

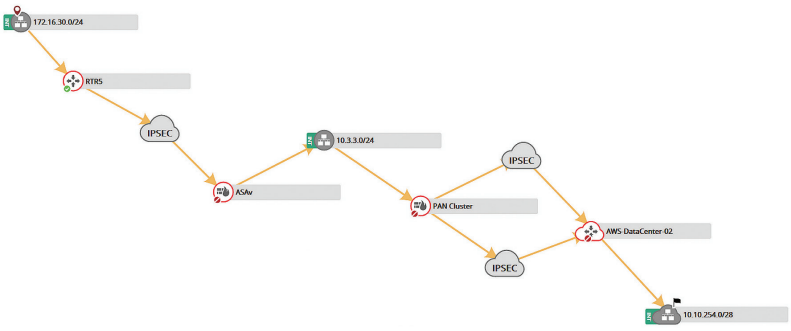
L'adoption du cloud se propage sur le plan géographique comme sectoriel et AWS est devenu le leader du marché IaaS (Infrastructure as a Service)1. La majorité des entreprises utilisent ou prévoient d'utiliser AWS afin de fournir de nouveaux services et applications à leurs clients avec une agilité accrue[2].

Alors que de nombreuses entreprises adoptent AWS pour héberger de nouvelles applications ou migrer celles existantes, il reste toujours des questions en suspens concernant la définition et la mise en œuvre des stratégies de sécurité sur AWS. Afin d'éviter des retards et d'atteindre l'agilité optimale avec AWS, les équipes de sécurité ne prennent souvent pas part aux modifications journalières en termes de sécurité et de connectivité, voire même à la configuration initiale des groupes de sécurité d'AWS.

Outre les défis liés à la visibilité et à l'application des stratégies sur AWS, la plupart des entreprises qui adoptent AWS possèdent toujours leurs propres infrastructures physiques et virtuelles, qu'ils continuent de gérer. Ces environnements hybrides composés de cloud public, de cloud privé et de réseaux physiques posent de nouveaux défis en matière de segmentation pour la visibilité, la sécurité et la connectivité au travers des fournisseurs et plateformes de sécurité réseau, et sont susceptibles de compromettre la sécurité, la mise en conformité liée aux réglementations, voire même la disponibilité des applications critiques.

Visibilité centralisée par l'intermédiaire d'AWS et des réseaux locaux

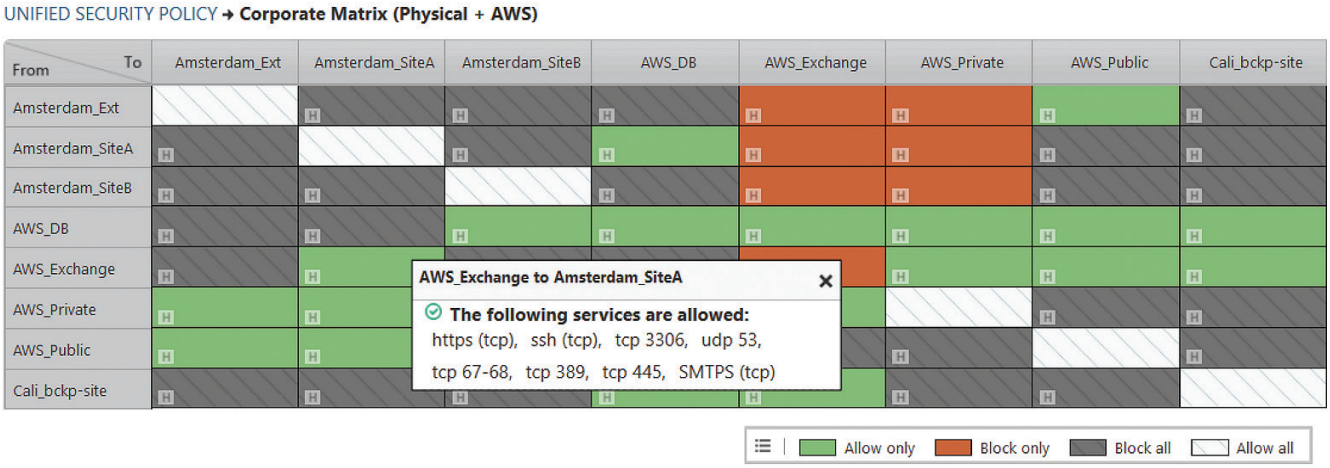
La visibilité est essentielle afin de pouvoir gérer la sécurité et la connectivité par l'intermédiaire des réseaux hybrides. Les équipes de sécurité et d'opérations réseau qui ne disposent d'aucune visibilité sur les groupes de sécurité et les règles AWS ne peuvent identifier ou vérifier les violations des politiques de sécurité. Grâce à Tufin, elles bénéficient d'une découverte automatique des instances AWS, des applications et de leur connectivité, des TAGs, ainsi que des groupes de sécurité et des règles associées et sont en mesure de surveiller les modifications en temps réel. Cette visibilité leur permet également de réaliser des analyses afin d'identifier toute violation des politiques de sécurité ou des réglementations sectorielles de l'entreprise. De plus, l'utilisation de plusieurs plateformes et fournisseurs à travers un réseau hybride complexifie considérablement la visualisation de la connectivité pour les applications hébergées sur AWS et sur l'infrastructure locale. Grâce à une gestion centralisée des plateformes cloud publiques et privées, ainsi que des pares-feux et routeurs physiques, Tufin offre une visualisation de la connectivité applicative permettant d'identifier et de résoudre les problèmes ou de planifier les modifications et migrations.



L'analyse topologique interactive de Tufin visualise la connectivité via les pare-feu AWS et locaux

Conformité aux politiques et vérification pour les applications AWS

Bien souvent, les contrôles de sécurité et de conformité définis et appliqués au niveau local ne le sont pas sur les plateformes cloud. Néanmoins, les applications hébergées sur AWS doivent être harmonisées avec les politiques de l'entreprise pour protéger les systèmes et données critiques et repousser la prochaine cyberattaque. Tufin permet aux clients de définir et d'appliquer une stratégie de sécurité unifiée (Unified Security Policy™) renforçant la segmentation réseau et garantissant la conformité constante aux normes internes et sectorielles telles que PCI DSS, SOX, HIPAA, NERC CIP et ISO 27001. La conformité permanente permet non seulement aux entreprises d'éviter les pénalités, mais également de réduire près de 70 % les efforts liés aux audits. Les équipes de sécurité peuvent éviter d'être contournées par les équipes cloud en adoptant un contrôle des politiques de sécurité intégré tout en n'entraînant aucun retard dans la mise à disposition des nouvelles applications et services.



Tufin Unified Security Policy renforce la segmentation inter-zones via AWS et le réseau hybride

Agilité optimisée grâce à l'automatisation de bout en bout

L'agilité est le facteur concurrentiel le plus critique du paysage commercial actuel. Toutefois, pour les applications nord-sud hébergées à la fois sur AWS et sur l'infrastructure locale, l'agilité peut être limitée par l'hétérogénéité des systèmes de gestion et d'orchestration. Une application peut être intégralement déployée sur AWS, mais devoir attendre l'accès à la base de données d'un Datacenter via des pare-feu et routeurs physiques avant d'être lancée. Grâce à la gestion centralisée et au processus de modification entièrement automatisé de Tufin, les clients peuvent mettre en œuvre les exigences de connectivité de bout en bout par l'intermédiaire des réseaux hybrides.

Les processus de modification opérés par Tufin s'intègrent à l'automatisation de l'analyse des risques avec une conformité continu des stratégies, de la conception et du déploiement pour les pare-feu et plateformes cloud, et de la vérification en vue d'optimiser la productivité et d'accélérer la mise en œuvre.

Tufin permet la mise en œuvre automatisée des modifications liées aux groupes de sécurité AWS et guide les utilisateurs vers le groupe de sécurité à modifier. Grâce à l'orchestration de bout en bout, Tufin offre également un processus automatisé pour la migration des applications vers AWS. Le modèle de connectivité applicative peut être dupliqué et déployé sur AWS via une interface utilisateur de type assistant, et l'application d'origine peut alors être mise hors service via le processus Tufin afin de renforcer la sécurité réseau.

Tufin® est leader dans le secteur de l'orchestration des politiques de sécurité réseau et compte parmi ses clients plus de la moitié des 50 premières entreprises du classement du Forbes Global 2000. Tufin simplifie la gestion des réseaux les plus vastes et les plus complexes au monde, constitués de milliers de pare-feux, d'éléments de réseau et d'infrastructures de cloud hybride émergentes. Primée, la solution Tufin Orchestration Suite™ est sollicitée par les entreprises afin d'accroître leur agilité face à l'évolution constante des exigences opérationnelles tout en maintenant un dispositif de sécurité puissant. Tufin réduit la surface d'attaque et répond à la nécessité d'avoir une plus grande visibilité sur une connectivité sécurisée et fiable des applications. Grâce à l'automatisation de la sécurité de leur réseau, les entreprises peuvent mettre en œuvre des modifications en quelques minutes avec une analyse proactive des risques et une conformité permanente aux politiques de sécurité. Tufin compte plus de 2 100 clients à travers le monde, tous secteurs confondus ; ses solutions et technologies sont protégées par des brevets aux États-Unis et dans d'autres pays.

1 Gartner Magic Quadrant for Cloud Infrastructure as a Service, Worldwide report, Lydia Leong et al, publié le 3 août 2016
2 RightScale 2016 State Of The Cloud Report

Tufin, Unified Security Policy, Tufin Orchestration Suite et le logo Tufin sont des marques commerciales de Tufin. Tous les autres noms de produits mentionnés ici sont des marques commerciales ou des marques déposées de leurs propriétaires respectifs.

Copyright © 2020 Tufin
SB-03-20