tufin The Security Policy Company. + aws

Gemeinsame Lösung im Überblick

Transparenz, Compliance und Automatisierung für Amazon Web Services (AWS)

Vorteile für Ihr Unternehmen:

- Umfassender Sicherheitsüberblick für AWS und das heterogene Netzwerk
- Höhere Agilität durch Orchestrierung von Sicherheitsrichtlinien für Cloud-Plattformen und lokale Umgebungen
- Integrierte Kontrollen dank automatisierter Sicherheitsmechanismen für AWS
- Enge Segmentierung und zuverlässige Einhaltung von Richtlinien in AWS und dem gesamten hybriden Netzwerk
- Verkürzung der Vorbereitungszeit für Audits um bis zu 70 % dank kontinuierlicher Compliance
- Problembehandlung und Bereitstellung von Verbindungen für „Nord-Süd"-Anwendungen

Cloud-Technologien gewinnen weltweit in allen Branchen stark an Bedeutung, und AWS gilt als eine der führenden Lösungen auf dem IaaS-Markt (Infrastructure-as-a-Service)1. Die Mehrzahl der Unternehmen nutzen oder planen die Nutzung von AWS, um neue Dienste und Anwendungen für ihre Kunden schneller und flexibler bereitstellen zu können.

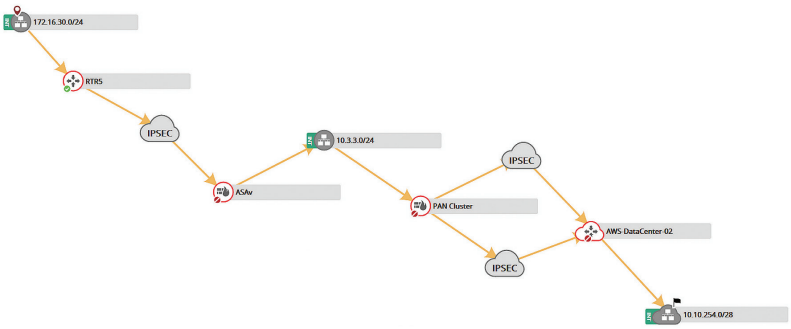
Viele Unternehmen setzen AWS ein, um neue Anwendungen zu hosten oder bestehende zu migrieren. Die Definition und Umsetzung von Sicherheitsrichtlinien in AWS ist allerdings nicht ganz unproblematisch. Um Abläufe zu beschleunigen und die Flexibilität von AWS voll auszuschöpfen, werden die Sicherheitsteams in die täglichen Änderungen an der Sicherheit und Konnektivität von AWS oft nicht einbezogen. Und selbst die Einrichtung von AWS-Sicherheitsgruppen läuft häufig an der Sicherheitsabteilung vorbei.

Doch nicht nur die Transparenz und Durchsetzung von Sicherheitsrichtlinien in AWS sind Herausforderungen. Die meisten Unternehmen, die AWS zu nutzen beginnen, müssen weiterhin auch vorhandene physische und virtuelle Infrastrukturen verwalten. Das Ergebnis sind heterogene Umgebungen aus öffentlichen und privaten Clouds sowie physischen Netzwerken mit verschiedenen Plattformen und Produkten zahlreicher Anbieter. Dies beeinträchtigt die Transparenz, Sicherheit und Konnektivität und kann den Sicherheitsstatus, die regulatorische Compliance und sogar die Verfügbarkeit geschäftskritischer Anwendungen erheblich gefährden.

Zentrale Übersicht über AWS und lokale Netzwerke

Sichtbarkeit ist eine unerlässliche Voraussetzung, um Sicherheit und Konnektivität in heterogenen Netzwerken zu gewährleisten. Wenn Sicherheits- und Netzwerkteams keinen Überblick über AWS-Sicherheitsgruppen und -regeln haben, können sie Richtlinienverstöße nicht feststellen und sich nicht angemessen auf Audits vorbereiten. Mit Tufin werden AWS-Instanzen, Anwendungen und Anwendungsverbindungen, Tags sowie Security-Groups und -regeln automatisch erfasst. Änderungen können in Echtzeit überwacht werden, sodass die Teams stets auf dem neuesten Stand sind. Diese Transparenz befähigt die Teams zudem, Analysen durchzuführen, um Verstöße gegen interne Sicherheitsrichtlinien oder Branchenstandards zu erkennen.

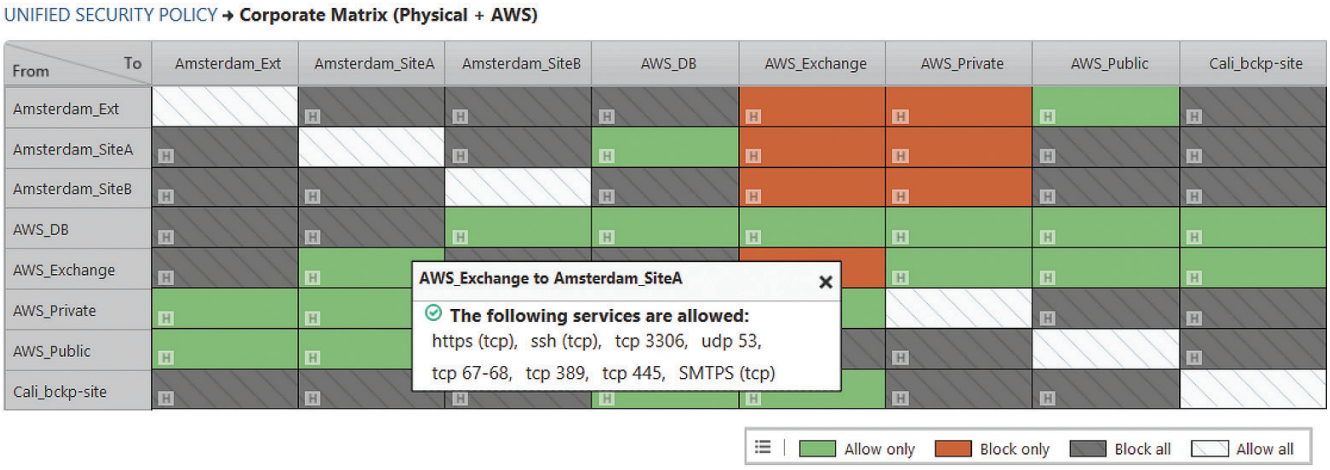
Ein weiteres Problem in hybriden Netzwerken, die mehrere Plattformen und Anbieter umspannen, ist die Visualisierung der Anwendungskonnektivität für AWS und die lokale Infrastruktur. Durch die zentrale Verwaltung von Public- und Private-Cloud-Plattformen sowie physischen Firewalls und Routern kann Tufin die Anwendungskonnektivität visuell darstellen. Diese Darstellungen erleichtern die Fehlerbehebung und die Planung von Änderungen und Migrationsvorhaben.



Tufins interaktive Analyse von Topologiepfaden zur Visualisierung der Konnektivität für AWS und lokale Firewalls

Richtlinienkonformität und Auditfähigkeit für AWS-Anwendungen

Lokal definierte und implementierte Sicherheits- und Compliance-Kontrollen werden in Cloud-Plattformen oft nicht durchgesetzt. Anwendungen, die in AWS gehostet werden, müssen jedoch den Richtlinien des Unternehmens entsprechen, damit sensible Systeme und Daten geschützt bleiben und Cyberangriffe jederzeit abgewehrt werden können. Tufin unterstützt die Kunden dabei, eine zentrale Unified Security Policy™ zu entwerfen und durchzusetzen, die für eine engere Netzwerksegmentierung sorgt und die laufende Einhaltung von internen Richtlinien und Branchenstandards wie PCI DSS, DSGVO, SOX, HIPAA, NERC CIP und ISO 27001 gewährleistet. Durch kontinuierliche Compliance vermeiden Unternehmen nicht nur Geldbußen für Verstöße, sondern können auch ihren Aufwand zur Vorbereitung auf Audits um bis zu 70 % senken. Und die Sicherheitsteams können vermeiden, von Cloud-Teams übergangen zu werden, indem sie eine integrierte Kontrolle für Sicherheitsrichtlinien implementieren, die die Bereitstellung neuer Anwendungen und Dienste nicht verzögert.



Zonenweise Segmentierung in AWS und im hybriden Netzwerk mit der Unified Security Policy von Tufin

Maximale Agilität dank durchgehender Automatisierung

In der modernen Geschäftswelt ist Agilität der wichtigste Wettbewerbsfaktor. „Nord-Süd"-Anwendungen, die sich über AWS und die lokale Infrastruktur erstrecken, sind jedoch aufgrund unterschiedlicher Verwaltungs- und Orchestrierungssysteme oft unflexibel. Eine Anwendung kann vollständig in AWS bereitgestellt werden, muss aber über physische Firewalls und Router auf eine Datenbank im Rechenzentrum zugreifen, bevor sie gestartet werden kann. Mit der zentralen Verwaltung und den vollautomatischen Änderungsprozessen von Tufin können die Kunden Konnektivitätsanforderungen im gesamten heterogenen Netzwerk umsetzen.

Der automatische Änderungsprozess von Tufin umfasst Risikoanalysen für integrierte Compliance, die Planung und Bereitstellung von Änderungen für Firewalls und Cloud-Plattformen sowie die Überprüfung der Änderungen. Die Automatisierung steigert die Produktivität und beschleunigt die Umsetzung.

Tufin stellt Änderungen für AWS-Sicherheitsgruppen automatisch bereit und hilft den Nutzern, die jeweils relevante Sicherheitsgruppe zu identifizieren. Auf Basis durchgehender Orchestrierung bietet Tufin auch einen automatisierten Prozess für die Migration von Anwendungen auf AWS. Das Modell für Anwendungskonnektivität kann mit einer Wizard-ähnlichen Benutzeroberfläche in AWS dupliziert und bereitgestellt werden. Um die Netzwerksicherheit zu erhöhen, kann die ursprüngliche Anwendung dann mit dem entsprechenden Tufin-Prozess außer Betrieb genommen werden.

Tufin® ist der Marktführer im Bereich Network Security Policy Orchestration und zählt 23 der DAX30 und mehr als die Hälfte der Top-50-Unternehmen in den Forbes Global 2000 zu seinen Kunden. Tufin vereinfacht die Verwaltung von Netzwerken, die zu den größten und komplexesten weltweit zählen und Tausende von Firewall- und Netzwerkgeräten sowie wachsende hybride Cloud-Infrastrukturen umfassen. Unternehmen entscheiden sich für die mehrmals ausgezeichnete Tufin Orchestration Suite™, um vor dem Hintergrund schnell veränderlicher Geschäftsanforderungen die Agilität zu erhöhen und gleichzeitig robuste Sicherheit aufrechtzuerhalten. Tufin verkleinert die Angriffsfläche und schafft die notwendige Übersicht, um sichere und zuverlässige Anwendungsverbindungen zu gewährleisten. Dank automatisierter Netzwerksicherheit können Unternehmen Änderungen innerhalb weniger Minuten umsetzen, dabei proaktive Risikoanalysen durchführen und die kontinuierliche Einhaltung von Richtlinien gewährleisten. Tufin betreut mehr als 2.100 Kunden aus allen Branchen und geografischen Regionen. Die Produkte und Technologien von Tufin sind in den USA und anderen Ländern durch Patente geschützt.
Weitere Informationen finden Sie auf **www.tufin.com.**

1 Gartner Magic Quadrant for Cloud Infrastructure as a Service, weltweiter Bericht, Lydia Leong et al, veröffentlicht am 3. August 2016
2 RightScale 2016 State Of The Cloud Report

Tufin, Unified Security Policy, Tufin Orchestration Suite und das Logo von Tufin sind Marken von Tufin. Alle anderen hier genannten Produktnamen sind Marken oder eingetragene Marken ihrer jeweiligen Eigentümer.

Copyright © 2020 Tufin
SB-03-20