tufin The Security Policy Company. + aws

Technology Partner Solution Brief

Visibility, Compliance and Automation for Amazon Web Services (AWS)

Benefits to Your Business:

- Gain security visibility into AWS and across the heterogeneous network
- Boost agility with security policy orchestration that runs across cloud and on-premises
- Automate security operations for AWS to establish built-in controls
- Ensure tight segmentation and policy compliance in AWS and across the hybrid network
- Reduce audit preparations by up to 70% with continuous compliance
- Troubleshoot and provision connectivity of north-south applications

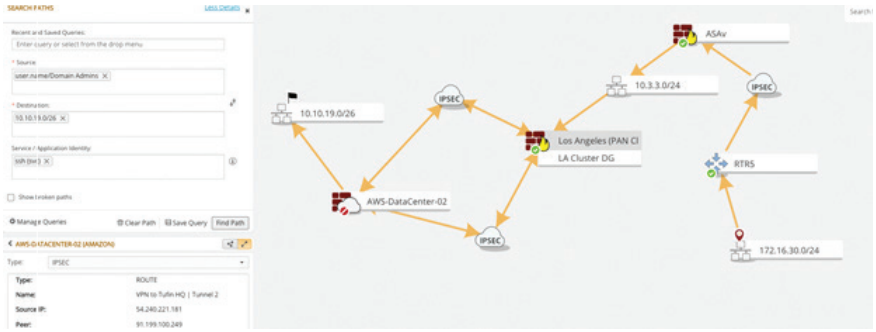
Cloud adoption is proliferating across geographies and industries and AWS has been named as a leader in the IaaS (Infrastructure as a Service) market[1]. Workload migration and cost optimization are the most common initiatives cited by global cloud decision makers and users.[2]

While many enterprises host new applications in AWS or migrate existing ones, there are still open questions around defining and enforcing security policies in AWS. In order to avoid delays and gain the optimal agility that AWS offers, security teams are often not involved in daily changes to the security and connectivity of AWS or even in the initial setup of AWS security groups.

In addition to challenges of visibility and enforcement in AWS, most enterprises that start using AWS still have physical and virtual infrastructure that they will continue to manage. These heterogeneous environments of public cloud, private cloud and physical networks raise challenges of split visibility, security and connectivity across vendors and platforms, and can significantly jeopardize security posture, regulatory compliance and even availability of mission critical applications.

Centralized Visibility Across AWS and On-Premises Networks

Visibility is essential to managing security and connectivity across the heterogeneous network. Security and network operations teams who have no visibility into AWS security groups and rules cannot identify policy violations or prepare for audits. With Tufin, they can run automatic discovery of AWS instances, applications and application connectivity, tags, security groups and rules, and stay up-to-date with real-time change monitoring. Based on this visibility they can also run analysis to identify violations to the organization's security policy or industry regulations.



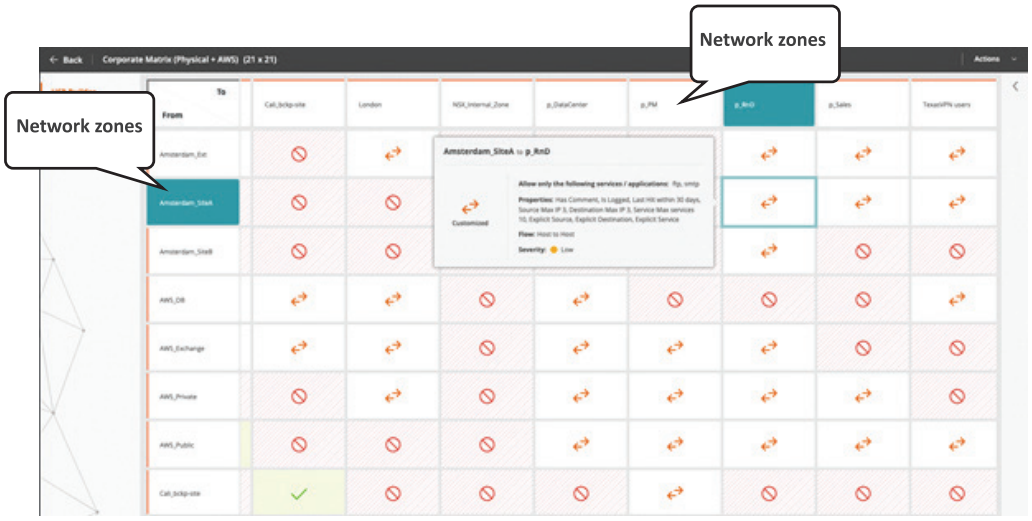
Tufin interactive topology path analysis visualizes connectivity across AWS and on-premises firewalls

In addition, using multiple platforms and vendors across the hybrid network makes it extremely difficult to visualize connectivity for applications that span AWS and on-premises infrastructure. By centrally managing public and private cloud platforms and physical firewalls and routers, Tufin can provide visualization of application connectivity that can be used to troubleshoot failure or plan changes and migrations.

tufin The Security Policy Company.

Policy Compliance and Audit Readiness for AWS Applications

Security and compliance controls that are defined and enforced on-premises are often not enforced in cloud platforms. Still, applications hosted in AWS must align with the organization's policies in order to protect sensitive systems and data and to contain the next cyberattack. Tufin helps customers define and enforce a central Unified Security Policy™ that tightens network segmentation and enforces continuous compliance with internal and industry standards like PCI DSS, GDPR, SOX, HIPAA, NERC CIP and ISO 27001. By enforcing continuous compliance, organizations not only avoid the penalties associated with failing to comply, but can also reduce their audit preparation efforts by up to 70%. Security teams can avoid being bypassed by cloud teams by adopting a built-in security policy control that does not delay the delivery of new applications and services.



Tufin Orchestration Suite Unified Security Policy –
Enforces zone-to-zone segmentation across AWS and the hybrid network

Maximized Agility with End-to-End Automation

Agility is the single most critical competitive factor in today's business landscape. However, for north-south applications that span across AWS and on-premises infrastructure, agility can be limited due to disparate management and orchestration systems. An application can be fully provisioned in AWS, but must await access to a data center database via physical firewalls and routers before it is launched. With Tufin central management and fully automated change process, customers can implement connectivity requirements end-to-end across the heterogeneous network.

The change process provided by Tufin includes in automated risk analysis for built-in policy compliance, automated design and provisioning for firewalls and cloud platforms, and automated verification to boost productivity and accelerate delivery.

Tufin delivers automated provisioning for changes to AWS security groups and guides users to target the right security group to be changed. Based on end-to-end orchestration, Tufin also provides an automated process for application migration to AWS. The application connectivity model can be duplicated and provisioned in AWS with a wizard-like user interface, and the original application can then be decommissioned with the Tufin process to increase network security.

tufin The Security Policy Company.

Tufin (NYSE: TUFN) simplifies management of some of the largest, most complex networks in the world, consisting of thousands of firewall and network devices and emerging hybrid cloud infrastructures. Enterprises select the company's Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. The Tufin Orchestration Suite reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. With over 2000 customers since its inception, Tufin's network security automation enables enterprises to implement changes in minutes instead of days, while improving their security posture and business agility.
Find out more at **www.tufin.com**.

1 Gartner, Magic Quadrant for Cloud Infrastructure & Platform Services, Raj Bala, Bob Gill, Dennis Smith, David Wright, Kevin Ji, 1 September 2020.
2 Flexera 2020 State of the Cloud Report