tufin The Security Policy Company. + paloalto NETWORKS®

Technology Partner Solution Brief

Network Security Policy Orchestration for Palo Alto Networks Next-Generation Firewall

Benefits to Your Business:

- Boost productivity with zero-touch automation for Panorama device group policy changes
- Leverage Tufin's advanced analysis and automation for Palo Alto Networks App-ID™, User-ID™ and Content-ID™
- Gain visibility and control of security and connectivity across hybrid networks
- Reduce attack surface by effectively managing segmentation and optimizing firewall and device group policies
- Implement network security changes in minutes instead of days with baked-in security
- Ensure continuous compliance and audit readiness

Palo Alto Networks® and Tufin® Provide Secure, Manageable and Compliant Environments

Enterprise IT and security experts are under increasing pressure to respond to complex network changes and keep up with growing business demands. Lack of network visibility hinders the ability to deliver services and applications with the security, speed and accuracy required. Together, the Tufin Orchestration Suite™ and Palo Alto Networks® Next-Generation Firewall provide advanced network protection and visibility, enabling agile and risk-free policy modifications. Using advanced analysis and automation technologies, the change processes are orchestrated across heterogeneous networks, devices, servers and applications, leveraging Palo Alto Networks Next-Generation Firewall capabilities.

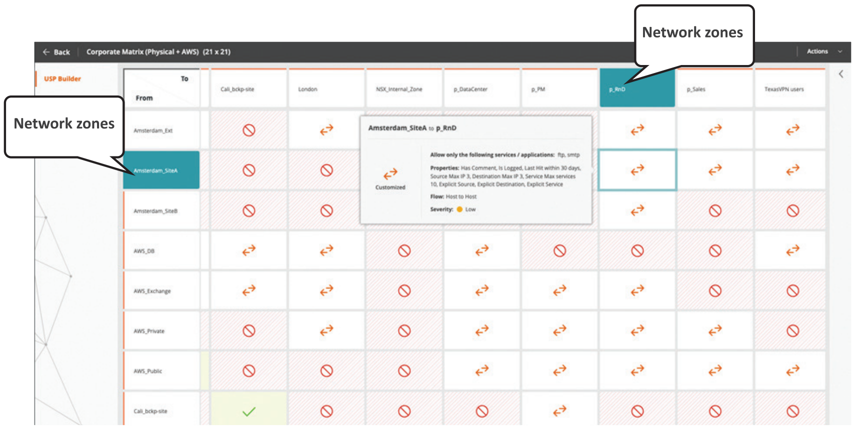
The Tufin Orchestration Suite is a complete solution for automatically designing, provisioning, analyzing and auditing network security changes from the application layer down to the network layer. Tufin's solution provides management and change automation for Palo Alto Networks Next-Generation Firewalls directly or managed through Palo Alto Networks Panorama.

Automatic Network Security Change Design and Implementation Based on Application Identity

The Palo Alto Networks-Tufin solution significantly shortens the time previously required to make network security changes with zero-touch automation. Automation is based on cutting-edge network topology simulation analysis that identifies the target Panorama device group policies, taking into consideration hierarchies as well as Application-IDs, User-IDs and Content-IDs, in complete alignment with Palo Alto Networks best practices. Then a detailed change plan is suggested and, once approved, deployed to the relevant Panorama device group policies.This ensures a quick and accurate process to grant the required application connectivity while complying with the organization's security policy.

Gain Insight and Control Over Complex Networks

Understanding and enforcing network segmentation is a major challenge for IT experts. Tufin's Security Zone Matrix simplifies this task by visually mapping the desired network zone-to-zone traffic flow and instantly providing detailed insights on your network segmentation, including what services are allowed between different network zones and zone sensitivity across physical, virtual and hybrid Palo Alto networks. Tufin orchestration suite also provides real-time monitoring of policy changes across heterogeneous environments, with enhanced visibility for Palo Alto security policies allowing control over tags, security profiles and log profiles.



Corporate Matrix (Physical + AWS) (21 x 21)

To / From	Cali_bckp-site	London	NSX_Internal_Zone	p_DataCenter	p_PM	p_RnD	p_Sales	TexasVPN users
Amsterdam_Ext	⊘	⇄				⇄	⇄	⇄
Amsterdam_SiteA	⊘	⊘				⇄	⇄	⇄
Amsterdam_SiteB	⊘	⊘				⇄	⊘	⊘
AWS_DB	⇄	⇄	⊘	⇄	⊘	⊘	⊘	⇄
AWS_Exchange	⇄	⇄	⊘	⇄	⇄	⇄	⊘	⊘
AWS_Private	⊘	⇄	⊘	⇄	⇄	⇄	⇄	⊘
AWS_Public	⊘	⊘	⊘	⇄	⇄	⇄	⇄	⇄
Cali_bckp-site	✓	⊘	⊘	⊘	⇄	⊘	⊘	⊘

Amsterdam_SiteA to **p_RnD**

⇄ Customized

Allow only the following services / applications: ftp, smtp

Properties: Has Comment, Is Logged, Last Hit within 30 days, Source Max IP 3, Destination Max IP 3, Service Max services 10, Explicit Source, Explicit Destination, Explicit Service

Flow: Host to Host

Severity: ● Low

Tufin Orchestration Suite Unified Security Policy – enables central management of network segmentation to ensure continuous compliance

Proactive Risk Analysis and Impact Simulation

Every change made to the Panorama device group or firewall policies is a potential threat to data security and application availability. Simulating the impact of a change is virtually impossible without the proper tools. As part of the automated change process, Tufin Orchestration Suite proactively checks every access request against the desired corporate security policy and internal compliance policies to identify and flag potential violations. The same proactive analysis is applied to application connectivity changes to ensure that applications are in compliance with internal and industry regulations.

Optimize Your Firewalls to Reduce Attack Surface

Tufin Orchestration Suite helps enterprises to optimize next generation firewalls across heterogeneous environments with:

- Optimization of next-generation Panorama device group and firewall policies by identifying rules and objects that are misconfigured, risky or unused, including unused users and applications.
- Automated process for decommissioning rules that are unused or otherwise obsolete
- Recommendations for aligning next-generation firewall policies with industry best practices
- Firewall analysis and reporting tools that enable security teams to achieve better productivity
- Built-in, customizable workflows for network and firewall changes

Continuous Regulatory Compliance with Industry Standards

Tufin Orchestration Suite provides a closed-loop process for enforcing, verifying and documenting compliance with industry standards such as PCI DSS, GDPR, NERC CIP and SOX. Every firewall policy change is evaluated before implementation ensuring safe deployment ahead of time. In addition, manual changes that can lead to compliance violations are detected automatically, and a resolution fix plan is suggested.

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**.

paloalto NETWORKS®

Palo Alto Networks is the next-generation security company, leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, our game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization's most valuable assets. Find out more at www.paloaltonetworks.com