

Palo Alto Networks and Tufin

Network Security Policy Management

Benefits of the Integration

Together, Palo Alto Networks and Tufin provide:

- Insight, visibility, and control for complex networks
- Continuous network compliance assurance and auditability with industry standards
- Automated network security change design and provisioning based on App-ID, User-ID, and Content-ID
- Proactive risk analysis and impact simulation
- Unified security policy across heterogeneous platforms
- Optimization of Palo Alto Networks NGFW policies

The Challenge

Enterprise IT and security experts are under increasing pressure to manage complex network environments and keep up with growing business demands. In this dynamic and evolving business environment, lack of centralized visibility into network security hinders an organization's ability to deliver services and applications with the required security, speed, and accuracy.

Managing such diverse and complex environments poses significant challenges, and it adversely affects the service-level agreements (SLAs) of the IT and security teams to implement simple changes to the network. Time spent analyzing the impact of the smallest change to the network and applications takes away the focus from important projects in your data centers. Combine this with the steady stream of various audit and compliance requests, and the strain on resources is even further magnified.

Tufin Orchestration Suite

Tufin Orchestration Suite™ is a complete solution for automatically designing, provisioning, analyzing, deploying, and auditing network security changes from the application layer down to the network layer. It provides management and change automation for Palo Alto Networks Next-Generation Firewalls (NGFWs) directly or through Palo Alto Networks Panorama™ network security management. Using advanced analysis and automation features, change processes are orchestrated across heterogeneous networks, devices, servers, and applications by taking advantage of Palo Alto Networks NGFW capabilities.

Palo Alto Networks

Palo Alto Networks NGFWs offer a prevention-focused architecture that is easy to deploy and operate. Automation reduces manual effort so your security teams can replace disconnected

tools with tightly integrated innovations, focus on what matters, and enforce consistent protection everywhere.

Palo Alto Networks NGFWs inspect all traffic, including all applications, threats, and content, and tie that traffic to the user, regardless of location or device type. The user, application, and content—the elements that run your business—become integral components of your enterprise security policy. As a result, you can align security with your business policies as well as write rules that are easy to understand and maintain.

Palo Alto Networks and Tufin

Together, the Tufin Orchestration Suite and Palo Alto Networks NGFWs provide a comprehensive application- and user-aware change management and automation platform to help organizations achieve and maintain secure, compliant environments.

Tufin Orchestration Suite provides the ability to automate network security change design and provisioning based on Palo Alto Networks App-ID™, User-ID™, and Content-ID™ technology. The Tufin abstraction layer provides visibility over the heterogeneous network to eliminate the complexity of separately managing multiple vendors and their devices. The consolidated management enables automated proactive risk analysis and impact simulation of network changes.

Tufin Orchestration Suite enables you to operationalize your security policy through a zone-to-zone-based connectivity matrix to ensure compliance against security policy across Palo Alto Networks security solutions as well as third-party vendors and their devices. Through policy aggregation and enrichment, Tufin enables you to analyze policy across Palo Alto Networks solutions to identify unnecessary or risky access and achieve policy health.

Use Case No. 1: Firewall Operations Optimization

Challenge

A network comprising multiple vendors, platforms, and network security devices makes it difficult to understand and optimize network topology, complicating the design of secure and accurate new access policies.

Answer

Capitalize on your existing network security investments and manage network security changes agnostic of vendors through network security policy management. Leverage Palo Alto Networks NGFW features adjacent to the management of your legacy firewall, software-defined network (SDN), and public cloud. This gives you the ability to achieve accurate change automation from analysis, risk assessment, change design, change provisioning, and change validation and reporting across your network.

Benefits

Together, Tufin and Palo Alto Networks NGFW features provide end-to-end, policy-driven automation and orchestration across an enterprise network.

Use Case No. 2: Assure Compliance and Audit Readiness

Challenge

Many organizations are unable to quickly assess the gaps between their current and desired state of compliance, leading to prolonged audit processes and uncertainty around passing third-party reviews.

Centrally manage policies in Panorama on-premises and within SDN, alongside third-party network security devices and hybrid cloud

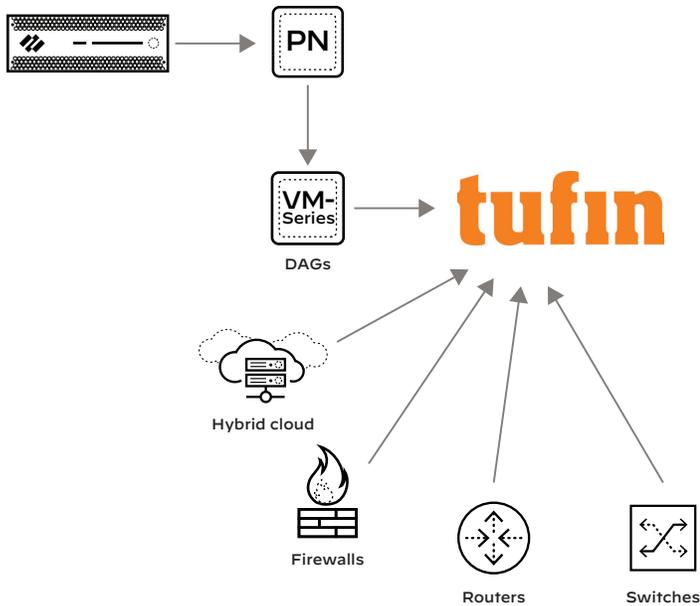


Figure 1: Palo Alto Networks and Tufin Orchestration Suite integration

About Tufin

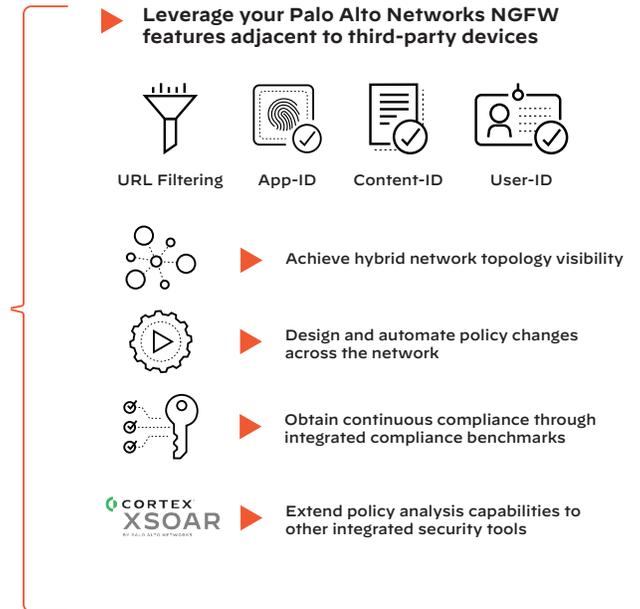
Tufin® is the leader in Network Security Policy Orchestration, serving more than half of the top 50 companies in the Forbes Global 2000. Tufin simplifies management of some of the largest, most complex networks in the world, consisting of thousands of firewall and network devices and emerging hybrid cloud infrastructures. Enterprises select the award-winning Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. Tufin reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. Its network security automation enables enterprises to implement changes in minutes with proactive risk analysis and continuous policy compliance. Tufin serves over 2,100 customers spanning all industries and geographies; its products and technologies are patent-protected in the U.S. and other countries. Find out more at www.tufin.com.

Answer

Deploy an integrated zone-to-zone-based connectivity matrix that reflects regulatory mandates and your corporate security policies to identify existing violations, then use it as a benchmark to assess the risk of requested changes and compliance violations.

Benefits

Obtain a measurable and continuous state of compliance against your compliance requirements and automate reporting based on all Tufin metadata-enriched policy data.



About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.



3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000

Sales: +1.866.320.4788

Support: +1.866.898.9087

www.paloaltonetworks.com

© 2020 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. palo-alto-networks-and-tufin-tpb-072820