

Tufin Orchestration Suite

Network Security Policy Orchestration

Balancing business agility and security across heterogeneous, physical networks and hybrid cloud platforms

As the market-leading provider of Network Security Policy Orchestration, Tufin takes a policy-based approach to automate change requests to boost security and increase agility for the world's largest organizations and most complex networks. From the application to the firewall, Tufin unifies security policy and provides advanced automation capabilities to increase business agility, eliminate errors from manual processes, and ensure continuous compliance.

Agility and Security with Network Security Policy Orchestration:



Implement security changes in minutes instead of days

- Boost agility with end-to-end change automation across vendors and platforms
- Increase productivity and avoid errors with zero-touch automation for change design, provisioning and verification
- Ensure business continuity by managing application connectivity across the heterogeneous network



Ensure continuous compliance with security standards

- Eliminate security violations with proactive risk analysis and automatic decommissioning of risky and redundant rules
- Reduce audit preparation time by up to 70%
- Simplify compliance with industry regulations such as PCI DSS, GDPR, HIPAA, SOX and NERC CIP



Reduce complexity of managing hybrid networks

- Manage security policies across enterprise firewalls, private and public cloud from a single pane of glass
- Ensure network and application connectivity with accurate topology map and analysis
- Reduce the attack surface with centralized control for network segmentation

Tufin helps solve the challenges of today's enterprise network:



Complexity



Change



Cybersecurity

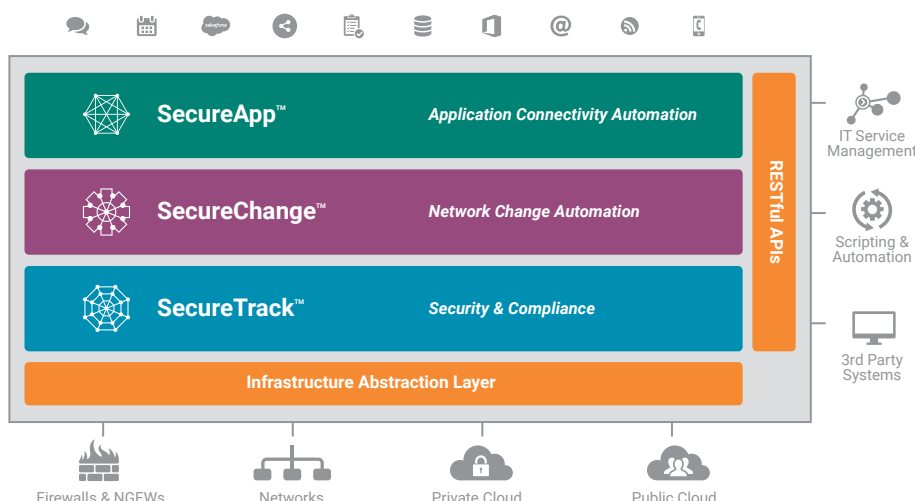


Compliance



Connectivity

Tufin Orchestration Suite™



“Implementing small changes now takes us about five minutes, larger changes about half an hour, depending on the size and complexity of the change. We plan changes with Tufin and it's much easier to perform server decommissioning according to policy with the policy analyzer.”

Network Security Administrator
Fujitsu TDS GmbH

End-to-End Security Change Automation

Automate access changes across enterprise firewalls and hybrid cloud platforms to increase productivity and eliminate misconfigurations. The change process is configurable and fully documented and includes proactive risk analysis, optimized change design, automated provisioning and access verification.

Unified Security Policy

Define and enforce a central zone-based segmentation matrix to strengthen the security posture and meet regulatory mandates. The Unified Security Policy matrix can be configured as a blacklist and/or whitelist and accommodate zones based on IP address or security groups. It provides a central console for identifying and addressing risky access across vendors and platforms, and also allows running proactive risk analysis for access changes.

The screenshot displays a 'Zone Matrix' with columns for 'From' and 'To' and rows for various zones: Amsterdam_Est, Amsterdam_SiteA, Amsterdam_SiteB, London, p_DataCenter, p_PM, p_RnD, p_Sales, TexasVPN users, and Toronto. Below the matrix, two pop-up windows show rule properties. The first window, titled 'The following services are blocked', lists rules for blocking traffic to 'p_Sales to Amsterdam_SiteB'. The second window, titled 'The following services are allowed', lists rules for allowing traffic from 'Amsterdam_SiteB to p_RnD'. Both windows include a 'Rule properties' section with bullet points such as 'Rules must have explicit source (not ANY)', 'Rules must have explicit destination (not ANY)', and 'Rules must have comment'.

Enterprise-wide Unified Security Policy Zone Matrix

Compliance and Audit Readiness

Ensure compliance with corporate security policies and external/industry regulations with a central console for real-time change tracking, including who made the change, when and why, a complete audit trail and audit-ready reports. Tufin security change automation also enforces compliance via proactive risk analysis for every access request, and via automated change authorization and verification.

A Single Pane of Glass for Managing Security Policy

Gain visibility and control for security policies and network connectivity across physical networks and hybrid cloud platforms. Tufin central console provides policy analysis, search and optimization capabilities across vendors and platforms. It also facilitates connectivity analysis and troubleshooting through an accurate, interactive topology map of the next generation network.

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 2,000 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.

The management team is happy with Tufin. They get fewer complaints that the change process is too slow, and they gain visibility into the growing amount of changes, the level of complexity of the changes (a typical change includes 10-15 new connections for a single application), and the process bottlenecks.

Network Operations Expert
RWE Supply & Trading (RWEST)

Technology Partners & Integrations

