tufin The Security Policy Company. + CISCO

Technology Partner Solution Brief

# Security Policy Orchestration for Cisco Firewalls and Security Management Products

## Benefits to Your Business:

- Implement network security changes in minutes with end-to-end automation across the hybrid network
- Boost productivity and avoid errors with zero-touch automation for managing ACLs
- Optimize Cisco ACLs with automated rule and object decommissioning
- Reduce the attack surface with centralized control for network segmentation
- Ensure business continuity by minimizing network and application downtime
- Enforce continuous compliance with enterprise and industry regulations
- Reduce audit preparation time by up to 70%
- Manage security policies across network firewalls, private and public cloud through a single pane of glass

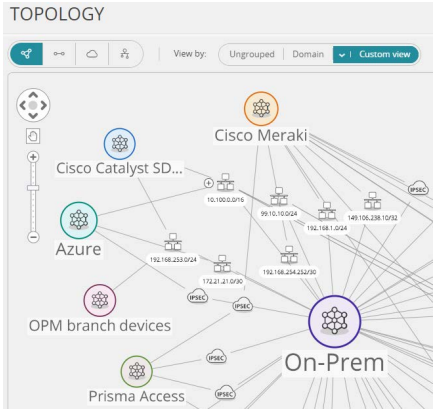
## Cisco® and Tufin® Ensure Manageability, Security and Compliance

Enterprise IT and security experts are under increasing pressure to manae growing network complexity and keep up with the business demands of digital transformation. A lack of visibility hinders an organizations ability to deliver services and applications with security, speed and accuracy. Together, Tufin Orchestration Suite™ with Cisco® Firewalls, Security Management and Networking products provide advanced network protection and visibility, enabling agile and risk-free policy modifications. Using advanced analysis and automation technologies, network security changes are orchestrated across heterogeneous networks and cloud platforms.

Tufin Orchestration Suite is a policy-based solution for automatically designing, provisioning, analyzing and auditing network security changes from the application level down to the networking level. Enterprises using Cisco ASA, Cisco iOS, Cisco Firepower, Cisco Meraki and Cisco Catalyst SD-WAN can leverage Tufin advanced policy-based security automation to increase business agility, eliminate errors from manual processes, and ensure continuous compliance. Tufin also offers advanced integration with Cisco ACI and Cisco Cisco switches and routers.

## Automatic Network Security Change Design and Provisioning

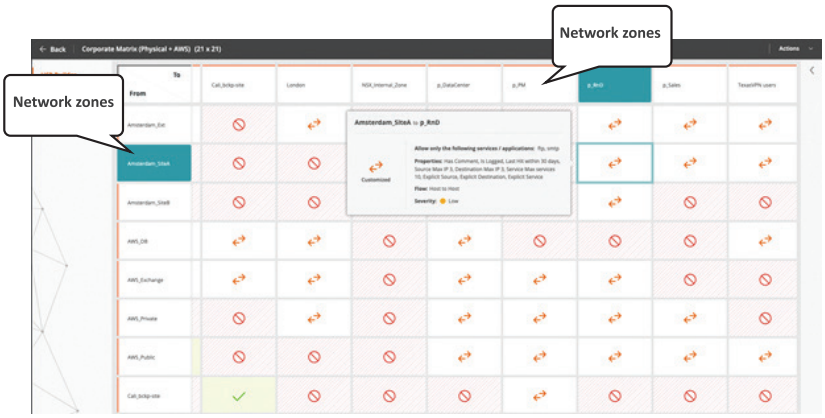
Tufin Orchestration Suite significantly shortens the time to make network security changes to Cisco ACLs through automated design and implementation. Change automation includes proactive risk analysis to identify and approve/reject violations to the organization security policy and automated network topology analysis to identify the firewalls and routers that need to change. The Tufin solution designs your optimized change plan to specific ACLs and provides automated provisioning and verification of the changes. This ensures a quick and accurate process to grant the required application connectivity while maintaining security policy compliance.




Tufin's interactive topology map visualizes connectivity across the entire hybrid cloud

## Gain Insight and Control over Complex Networks

Properly segmenting the network is a major challenge for IT and security professionals. Tufin's Unified Security Policy simplifies this task by visually mapping the baseline zone-to-zone access limitations. This configurable matrix provides detailed insights into what traffic is allowed or not allowed between security zones, across physical, virtual and hybrid networks.




Tufin's Unified Security Policy - simplified, centralized control of your network and security policy management

## Proactive Risk Analysis and Impact Simulation

Every change made to the Cisco firewall configuration to provide connectivity may also increase the risk of cyberattacks that can access sensitive systems and data. 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 rule against your corporate security and internal compliance policies to identify and flag potential risks.

## Optimize Your Firewalls

**Tufin Orchestration Suite optimizes firewall policies across heterogeneous network and hybrid cloud platforms by:**

- Identifying and decommissioning risky and redundant rules and objects that are unused or misconfigured
- Aligning firewall policies with industry best practices
- Providing policy analysis and reporting that improves productivity of security teams
- Customizing change workflows to align with organizational standards
- Designating approved compliance violations as exceptions and tracking for recertification

## 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, SOX, HIPAA, and NERC CIP. Every firewall policy change is evaluated before implementation ensuring safe deployment. Manual changes that result in compliance violations are automatically detected and a resolution plan is suggested.

Tufin provides a single platform for network and cloud security teams to simplify the management of security policies across today's complex, multi-vendor hybrid networks. The platform gives some of the largest companies in the world the end-to-end visibility and automation tools necessary to swiftly provide new access, enable fast and secure application deployment, and ensure continuous compliance and audit readiness. Tufin's proven solutions help more than 2,000 customers across industries including healthcare, financial services, utilities, telecommunications and retail to quickly identify and mitigate network risks. For more information, please visit www.tufin.com.

Cisco (NASDAQ: CSCO) is the worldwide technology leader that has been making the Internet work since 1984. Our people, products, and partners help society securely connect and seize tomorrow's digital opportunity today. Discover more at newsroom.cisco.com and follow us on Twitter at @Cisco.