

# Fortinet and Tufin Integrated Security Solution

## Network Security Policy Orchestration for Fortinet Firewalls

### Fortinet and Tufin provide Secure, Manageable and Compliant Environments

Fortinet and Tufin have developed an integrated offering for comprehensive network security policy orchestration. Together, the Tufin Orchestration Suite with Fortinet FortiGate firewalls and FortiManager network security management products reduce attack surface for mitigation of cyber threats. The joint offering enables IT security teams to manage complex heterogeneous physical networks and cloud platforms through a single pane of glass, providing advanced visibility and risk-free policy modifications. Based on advanced analysis and automation technologies, network security policies are orchestrated across the enterprise networks, leveraging the advanced capabilities and unparalleled security protection of Fortinet FortiGate firewalls.

### Tufin Orchestration Suite Integrates with FortiManager

Network security changes require end-to-end analysis for risk and compliance, change management, documentation, authorization, audit trails and so forth. Tufin Orchestration Suite is a comprehensive solution for these challenges – for automatically managing, designing, provisioning, analyzing and auditing network security changes from the application layer down to the network layer. Tufin's solution provides management and network security change automation for Fortinet FortiGate firewalls through FortiManager network security management. This integration enables the addition of Fortinet FortiGate firewalls as part of the organization's network in a smooth and simple manner.

### Automatic Network Security Change Design and Verification

Tufin significantly shortens the time previously required to make network security changes by automating both design and implementation. Automation is based on cutting-edge network topology simulation that identifies the relevant devices affected and performs an analysis of each relevant firewall policy. Then a detailed change plan is suggested and, once approved, deployed to security and network devices. This ensures a quick and accurate process to grant the needed application connectivity while maintaining the network security policy.

#### Key Benefits

- Unparalleled security protection
- Single pane of glass for managing security policies across network firewalls, private cloud and public cloud
- Optimize security policies
- Reduce attack surface for mitigation of cyber threats
- Implement network security changes securely in minutes
- Assure business continuity by minimizing network and application downtime
- Enable continuous compliance with enterprise and industry regulations
- Improve security, compliance and business agility through firewall change automation.

## Gain Insights and Control over Complex Networks

Understanding network and cloud 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 across all platforms, including which services are allowed between different network zones and zone sensitivity, restricting unauthorized east-west traffic.

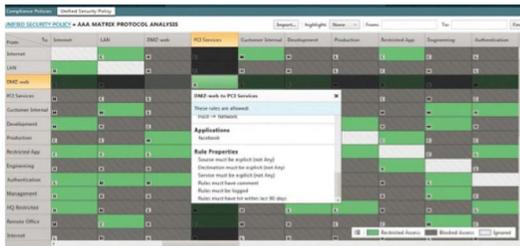


Figure 1: Tufin's Zone-Based Unified Security Policy Enables Policy Optimization and Network Segmentation and Reduces the Attack Surface.

## Optimize your Firewalls

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

- Optimization of policies by identifying rules and objects that are misconfigured, risky or unused
- Recommendations for aligning 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
- Integration with leading enterprise service management solutions, e.g., BMC Remedy and ServiceNow.

## Proactive Risk Analysis and Impact Simulation

Every change made to the firewall configuration 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 checks every access rule against your corporate security and internal compliance policies to identify and flag potential risks.

## Continuous Regulatory Compliance with Industry Standards

Tufin Orchestration Suite provides closed-loop process for enforcing, verifying and maintaining an automated audit trail for compliance with industry standards such as PCI DSS, SOX, and NERC CIP. Every firewall policy change is evaluated before implementation ensuring safe deployment ahead of time. In addition, manual changes that result in compliance issues are detected automatically and a resolution fix plan is suggested.

## About Tufin Orchestration Suite

Tufin Orchestration Suite™ is a complete solution for automatically managing, designing, provisioning, analyzing and auditing network security changes from the application layer down to the network layer. It minimizes errors and redoes for rapid service delivery, continuous compliance and business continuity. Tufin provides world-class network security policy orchestration solutions that enable organizations around the world to manage network configuration changes accurately and efficiently. By orchestrating complex processes involving multiple teams, applications, servers and network devices, Tufin addresses the challenges of a variety of stakeholders throughout the organization, while enabling them all to collaborate more effectively.