SOLUTION BRIEF

Fortinet and Tufin Security Solution

Network Security Policy Visibility and Automation for Complex, Hybrid Networks, Ensuring Continuous Compliance and Business Agility

Executive Summary

Gain comprehensive visibility, seamless automation, compliance, and risk assessment and mitigation with the joint solution from Tufin Orchestration Suite and the Fortinet Security Fabric, including FortiGate, FortiManager, FortiSIEM, and FortiSOAR across a complex, hybrid environment.

Challenges

Global organizations are consistently identifying means to maintain the balance between ensuring compliance, minimizing risk, and maximizing business agility. Effective visibility across an increasingly heterogeneous and hybrid network remains an elusive goal for many organizations. Lack of visibility into network topology and the security policies that govern network connectivity can leave organizations open to increased risk, making compliance exponentially more challenging and increasing the time to adequately triage and respond to a security incident.

Security policy change requests require careful design and review to ensure that each change meets business requirements, while simultaneously not introducing additional risk or compliance violations. Designing, reviewing, and approving these change requests is a largely manual process, which involves consulting numerous third-party data sources, documented security policies, and other resources for each request. As organizations move to a more agile business model, the number of change requests is growing exponentially.

Joint Solution

Tufin and Fortinet have partnered to deliver an industry-leading security solution to enable resource agility and fuel growth in organizations. The integration of the Tufin Orchestration Suite and Fortinet FortiGate, FortiManager, FortiSIEM, and FortiSOAR, enabled through the Fabric-Ready Program in the Fortinet Open Fabric Ecosystem, delivers unmatched security policy visibility, and change management in complex and heterogeneous environments, while maintaining continuous compliance and business agility.

Joint Solution Components

Tufin Orchestration Suite

Automate security policy visibility, risk management, provisioning, and compliance across multivendor, hybrid, and cloud environments. Eliminate the security bottleneck and increase the business agility of your organization.

Joint Solution Components

- FortiGate
- FortiManager
- FortiSIEM
- FortiSOAR
- Tufin Orchestration Suite

Joint Solution Benefits

- Fortinet Security Fabric platform for broad visibility and easy management of security and network operations across environments
- Unified dashboard for security policy management across diverse network firewalls, private cloud, and public cloud
- Automated change management for improved security, compliance, and business agility
- Efficient and effective security incident response with advanced network intelligence and automation
- Continuous compliance with enterprise and industry regulations
- Policy change requests enrichment with endpoint information and events, allowing more informed decisions and reduced risk

FORTINET FABRIC-READY

FortiGate

FortiGate next-generation firewalls (NGFWs) are network firewalls powered by purpose-built security processing units (SPUs) including the latest NP7 (Network Processor 7). They enable security-driven networking and are ideal network firewalls for hybrid and hyperscale data centers.

FortiManager

An integral part of the Fortinet Security Fabric, FortiManager supports network operations use cases for centralized management, best practices compliance, and workflow automation to provide better protection against breaches.

FortiSIEM

FortiSIEM brings together visibility, correlation, automated response, and remediation in a single, scalable solution. It reduces the complexity of managing network and security operations to effectively free resources, improve breach detection, and even prevent breaches.

FortiSOAR

Integrated into the Fortinet Security Fabric, FortiSOAR security orchestration, automation, and response (SOAR) remedies some of the biggest challenges facing cybersecurity teams today. Allowing security operations center (SOC) teams to create a custom automated framework that pulls together all of their organization's tools unifies operations, eliminating alert fatigue and reducing context switching. This allows enterprises to not only adapt but also optimize their security process.

Joint Solution Integration

The Tufin-Fortinet integrated solution empowers organizations with network security policy and topology visibility, continuous compliance, and the ability to manage routine change requests and security incidents more efficiently across a complex, hybrid environment.

Tufin leverages security policy and other network configuration information from FortiGate and FortiManager, along with other third-party devices, to provide organizations with a holistic view of the entire network ecosystem across private, public cloud, and hybrid environments. Security policy changes, both routine and in response to a security incident, can be optimized and automated by Tufin.

Tufin incorporates configuration management database (CMDB) and event data from FortiSIEM, unified compliance standards and best practices, as well as an accurate understanding of network topology to ensure continuous compliance and business agility throughout the change management life cycle. Changes can be automatically or manually provisioned by Tufin directly to FortiGate devices, or through FortiManager.

If a security incident does occur, Tufin's network visibility and change automation can be combined with FortiSOAR to make more intelligent automated incident handling decisions to implement effective and expedited threat containment actions.

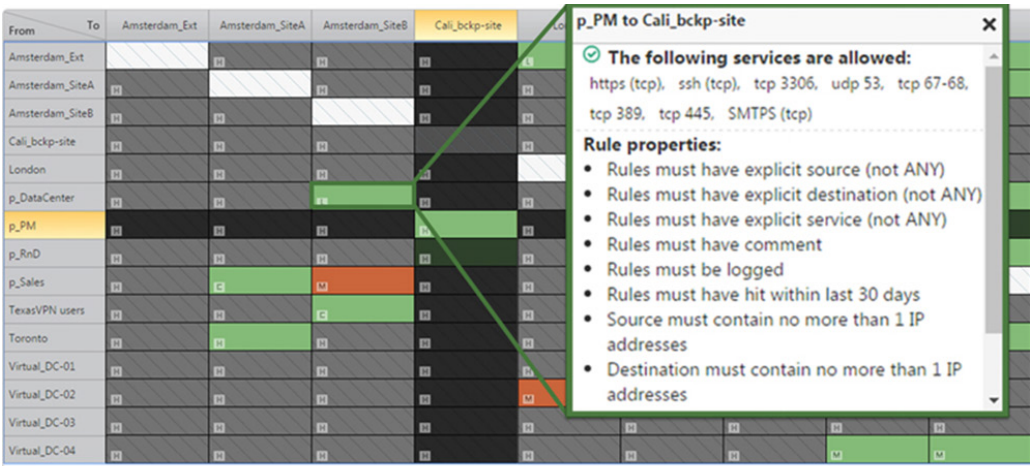

Figure 1: Tufin's zone-based Unified Security Policy enables policy optimization, network segmentation, and continuous compliance across a hybrid network.

Joint Use Cases

Use Case 1

Comprehensive Visibility Across the Hybrid Network—Tufin, combined with FortiGate and FortiManager, provides visibility across the entire hybrid network, providing a comprehensive understanding of network topology, global security policies, fine firewall features, and compliance with enterprise and industry regulations.

Use Case 2

Intelligent, Informed Change Management and Automation—Optimize security policies and ensure continuous compliance with Tufin. Incorporate FortiSIEM CMDB and event data into the change management process to make informed, intelligent, and recorded change decisions, reducing risk and the overall attack surface.

Use Case 2

Efficient and Effective Security Incident Response—Empower FortiSOAR with Tufin's complete network visibility and change automation. Utilize playbooks for routine and incident-based response including comprehensive information regarding network topology and security policy information and perform more effective containment of threats across the hybrid network.

About Tufin

Tufin (NYSE:TUFN) simplifies management of some of the largest, most complex networks in the world, consisting of thousands of firewalls 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 2,000 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.

May 10, 2021 3:53 PM

C:\Users\cyan\Documents\Creative Services - Misc\Document Edits\sb-fortinet-and-tufin-security-solution\sb-fortinet-and-tufin-security-solution-051021

849320-A-0-EN